УДК 004.75

С.В. Новиков, В.М. Зима, Д.В. Андрушкевич

ПОДХОД К ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ СЕТЕЙ ОБРАБОТКИ ДАННЫХ НА ОСНОВЕ ДОВЕРЕННОЙ ИНФРАСТРУКТУРЫ

Новиков С.В., Зима В.М., Андрушкевич Д.В. **Подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры.**
Аннотация. Предлагается подход к построению распределенных вычислительных сетей и организации защиты информации с использованием доверенной инфраструктуры. Отсутствие единой высокоуровневой платформонезависимой модели организации вычислительного процесса и защиты информации, а также необходимых механизмов, реализующих модель на уровне ее практического внедрения, порождает множество несогласованных между собой частных решений и приводит к неоправданному нагромождению технических и программных средств организации обработки информации в автоматизированных системах. Поэтому эволюционно развивающиеся системы, функционирующие на разных платформах в настоящее время, требуют внедрения доверенных решений в области защиты информации.
Ключевые слова: программные средства защиты информации, автоматизированная система, гетерогенная сеть, операционная система, доверенная среда, доверенная инфраструктура, прозрачное шифрование.

Novikov S.V., Zima V.M., Andrushkevich D.V. **Approach to Building Secure Distributed Networks of Data Processing based on Trusted Infrastructure.**
Abstract. An approach for building distributed computing networks and the organization of information security using trusted infrastructure is proposed. The lack of a single high-level platform-independent model of computing and information security, as well as the necessary mechanisms that implement the model at the level of its practical implementation raises many uncoordinated private decisions and leads to unnecessary pile of hardware and software organization of information processing of automated systems. Therefore, the evolutionary developing systems operating on different platforms currently require the implementation of trusted solutions in the field of information security.
Keywords: software data protection, automated system, a heterogeneous network, operating system, trusted environment, trusted in infrastructure, transparent encryption.

1. Введение. Информационные технологии сегодня развиваются столь стремительно, что уже трудно выделить сферу человеческой деятельности, в которой они не были бы востребованы. Любая современная организация, даже если она и не имеет удаленных филиалов, вовлекается в общий круг пользователей информационных услуг, в обязательном порядке использует глобальные коммуникации, имеет собственное виртуальное представительство в Сети, работает с современными средствами обмена данными в рамках собственного офиса. "Фактор Сети" незримо присутствует в управлении любого уровня и степени важности. В связи с этим проблема вовлечения Интернета в круг интересов любой организации, имеющей территориально распре-

деленную структуру, встает все острее. Не столько с точки зрения целесообразности такого шага, сколько с позиций обеспечения информационной безопасности, поскольку Сеть сегодня воспринимается часто как "агрессивное начало". Многие информационные системы являются уязвимыми к так называемым "внешним воздействиям". Сегодня уже пришло понимание того факта, что электронные средства хранения и передачи информации оказались даже более уязвимыми, чем обычные бумажные, так как их можно не только уничтожить, но и незаметно для владельца скопировать или изменить. Именно это является особо опасным для любой структуры.

Теми же проблемами обладают и каналы обмена данными. Мало того, что информация, в них циркулирующая, является по сути своей открытой и доступной для злоумышленника, так еще и сами средства обмена предоставляют последним возможность вторжения во внутренние ресурсы информационных систем. Понимая всю опасность, связанную с хранением и передачей данных по каналам связи, многие предприятия в мире расходуют на решение проблемы обеспечения информационной безопасности немалые средства. В России обеспечение информационной безопасности тоже превращается постепенно в общегосударственную проблему, так как "агрессивность" среды растет, внешние угрозы становятся все более изощренными. И хотя "фактор Сети" несколько преувеличен, опыт многих успешных внешних атак указывает на их немалую "внутреннюю" составляющую, тем не менее, игнорирование указанной проблемы может привести к невосполнимым потерям в управляемости каждой отдельно взятой структуры [1].

2. Проект доверенной инфраструктуры. Наличие развитой сетевой инфраструктуры на объектах гетерогенных, территориально распределенных автоматизированных систем (АС) является необходимым, но не достаточным условием создания интегрированного информационно-вычислительного пространства. Отсутствие единой высокоуровневой платформонезависимой модели организации вычислительного процесса и защиты информации, а также необходимых механизмов, реализующих модель на уровне ее практического внедрения, порождает множество несогласованных между собой частных решений и приводит к неоправданному нагромождению технических и программных средств организации обработки информации на объектах автоматизированных систем. Поэтому в настоящее время актуальными являются проблемы

разработки и внедрения, эволюционно развивающихся систем, функционирующих на различных платформах.

Одной из ключевых проблем создания доверенной среды в построении распределенных вычислительных сетей является решение вопроса о принципиальной допустимости и способах применения, в общем случае, недоверенных программно-аппаратных средств и компонентов в его составе. Объекты могут оснащаться разнородными аппаратно-программными платформами (АПП), функционирующими в составе защищенных центров обработки данных (ЦОД), выделенных специализированных серверов, а также рабочих станций. Неизбежным следствием при этом являются две возникающие задачи: интеграции разнородных информационно-вычислительных ресурсов и реализации унифицированной модели защиты процессов и данных в составе гетерогенных объектов. В статье предлагаются возможные технологии доверенной инфраструктуры, которая базируется на основе включения в АПП доверенного общесистемного программного обеспечения (ОСПО), в состав которого, наряду с компонентами интеграции разнородных приложений, обмена данными и управления вычислительным процессом, входят программные средства защиты информации. Также предложены возможные требования к организации доверенной среды путем создания доверенной инфраструктуры распределенных сетей обработки данных. Даны необходимые рекомендации по организации доверенной инфраструктуры критически важных объектов РФ.

На рисунке 1 представлена концепция доверенной инфраструктуры защищенных распределенных сетей. Таким образом, предлагается инфраструктура, которая будет состоять из контура, в состав которого будут входить: доверенный контроль, доверенный канал связи, доверенные сегменты распределенной сети, доверенные АРМ с различными платформами ОС, доверенное специальное программное обеспечение с НДВ, доверенная система шифрования, доверенная транспортная среда, доверенные администраторы всех сегментов сети, администратор доверенной инфраструктуры.

Для организации защиты информации на различных узлах распределенных сетей обработки данных предлагается введение данного контура с администраторским управлением на каждом сегменте контура, под управлением администратора доверенной инфраструктуры.

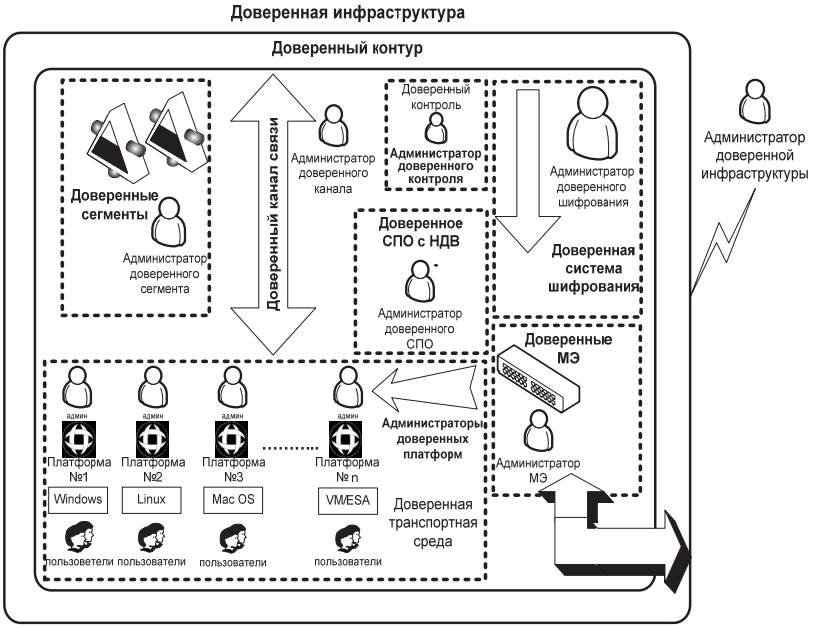

Рис. 1. Проект доверенной инфраструктуры защищенных распределенных сетей

В данной статье авторы предлагают рассмотреть некоторые из подходов защиты сегментов доверенной инфраструктуры, а именно:

- организацию защиты информации в доверенном контуре на различных платформах ОС;
- доверенные элементы распределенной информационной системы;
- двухуровневое шифрование в доверенной инфраструктуре;
- организация защиты контура в доверенной инфраструктуре.

3. Организация защиты информации в доверенном контуре на различных платформах ОС. Реализация унифицированных средств защиты в общем случае может достигаться применением организационных, технических и программных решений, а также их комбинацией. Причем применение технических средств защиты информации, разработанных для неоднородных программно-аппаратных платформ, в силу их ориентации на конкретные (специфические) интерфейсы используемого оборудования не может рассматриваться в качестве унифицированного решения проблемы. Поэтому унифицированные решения следует формировать на базе программных средств защиты (ПСЗ) информационных ресурсов, которые могут являться дополнением к уже

имеющимся в составе системы аппаратным (техническим) и программно-аппаратным средствам, а также осуществляемым мероприятиям организационного характера. Очевидно, что ПСЗ должны обеспечивать управление безопасностью при операциях с информационными объектами высших уровней абстракции (приложений уровня конечных пользователей, систем обмена данными, документооборота, приложений баз данных) [2].

Широко используемые в настоящее время программные компоненты защиты информации либо встраиваются в состав различных операционных систем (ОС) — встроенные ПСЗ — непосредственно разработчиками, либо подменяют собой стандартные обращения к объектам защиты (файлам, устройствам, исполняемым модулям) уровня ОС со стороны прикладных процессов (внешние ПСЗ). Недостатком применения встроенных ПСЗ является существенная зависимость построенной модели защиты от частных особенностей реализации разработчиком ОС средств управления безопасностью. При применении внешних ПСЗ возникает необходимость стабилизации (неизменности программной среды) конкретной версии используемой ОС. Поэтому для защиты объектов такого уровня должны использоваться унифицированные ПСЗ, служащие дополнением к недостающим механизмам защиты на уровне разнородных операционных систем и сетевых приложений [3].

Определим место унифицированных ПСЗ в общей архитектуре программного обеспечения объекта АС, имея в виду, что рассматриваемые ПСЗ предназначены для реализации унифицированной модели защиты в условиях изначальной неоднородности множества программных и технических компонентов, составляющих корпоративную сеть организации. В этих условиях унификация модели защиты на уровне разнородных элементов данного множества может достигаться средствами "промежуточного" слоя (middleware). Он образуется распределенными однородными (с точки зрения интерфейсов и выполняемых функций) компонентами общесистемного программного обеспечения (ОСПО), функционирующими под управлением всех операционных систем (базовых ОС), используемых в составе объекта АС. Указанное свойство является принципиальным отличием данного решения от большинства известных реализаций.

Перейдем от рассмотрения проблем защищенного функционирования отдельных средств вычислительной техники (СВТ) к проблемам защиты коммуникаций. Здесь в первую очередь следует отметить недостаточность применяемых в настоящее время средств фильтрации входящих/исходящих потоков данных между узлами вычислитель-

ных на сетевом уровне без адекватного решения проблемы безопасного взаимодействия конечных абонентов/приложений на прикладном уровне с использованием различных (разнородных) протоколов передачи данных [4]. В результате для гетерогенных корпоративных вычислительных сетей администратор безопасности, располагает набором разнородных инструментальных средств, в общем случае неадекватных решаемой проблеме.

Попытки практической реализации комплекса мер по обеспечению защиты информации на объекте путем использования предлагаемых программных продуктов различных классов наталкиваются на ряд противоречий концептуального характера. Они преимущественно связаны с неадекватностью имеющегося в распоряжении администратора безопасности набора инструментальных средств решаемым задачам по отображению избранной модели защиты на множество разнородных объектов вычислительной техники, сетевых средств и программного обеспечения различных производителей. Например, имеющиеся различия в используемых понятиях и формулируемых критериях информационной безопасности на уровне компьютерной лексики и терминов нормативных (регламентирующих) документов, определяющих политику безопасности для АС, создают проблему адекватного отображения нормативного уровня на уровень вычислительных систем. На рисунке 2 показана организация доверенной (защищенной) общесистемной транспортной среды в доверенной инфраструктуре [4].

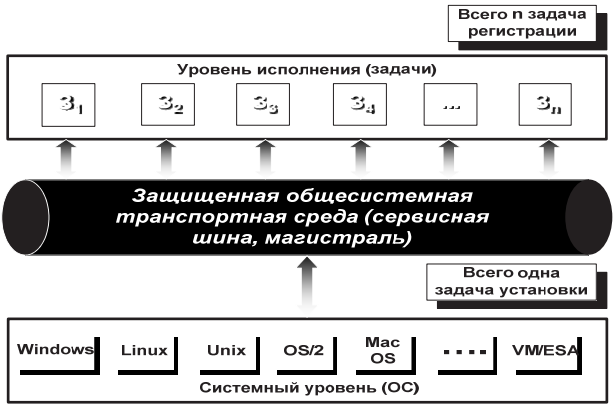

Рис. 2. Доверенная транспортная среда

Кроме того, существуют конструктивные различия в базовых средствах защиты информации уровня операционных систем и сетевых приложений различных производителей (IBM, Microsoft, SUN и др.),

отсюда — дополнительные сложности в реализации непротиворечивой модели защиты для гетерогенной вычислительной среды.

Необходимо отметить, что даже при проектировании вычислительных сетей, состоящих из однородного программного обеспечения и технических средств, использование одних только базовых средств защиты на уровне выбранной ОС оказывается недостаточным. Это происходит из-за наличия на уровне АС новых общесистемных свойств, затрагивающих принципы адресации ее элементов (системы как единого целого, объекта в составе территориально распределенной системы, ЛВС в составе объекта, вычислительного модуля в составе ЛВС, прикладной задачи в составе модуля), выбора атомарных единиц обмена данными, перечня защищаемых ресурсов и т. д. [5].

При непосредственном использовании компонентов защиты уровня отдельной ОС для решения задач создания территориально распределенных корпоративных вычислительных сетей и последующей обработки информации в контуре доверенной инфраструктуры возникают противоречия, к основным из которых можно отнести следующие:

1) базовые средства защиты информации на уровне ОС обеспечивают подключение пользователя к ресурсам отдельной ЭВМ, являющейся в общем случае лишь элементом в составе ЛВС (но не объекта в составе автоматизированной системы). В то же время на уровне АС необходим дополнительный, более важный с точки зрения вопросов безопасности этап: подключение пользователя-должностного лица к ресурсам информационной системы в соответствии с принятыми в АС соглашениями по адресации объектов, АРМ или отдельных программ. Это может относиться к отдельной программе, группе программ в АРМ, пользователю, группе пользователей и объекту в целом;

2) базовые средства защиты информации с точки зрения системы хранения на уровне ОС рассматривают файл в качестве элементарной единицы защиты данных. В то же время на корпоративном уровне АС единицами системы электронного документооборота являются формализованные сообщения, а также именованные в соответствии с общесистемными классификаторами документы. И то, и другое, как правило, не хранится в системе в виде отдельных файлов, более того, различные АС используют свои (как правило, с применением СУБД) специфические методы отображения множества элементов системы документооборота на файловые структуры;

3) средства защиты информации в составе ОС управляют доступом на уровне реальных (физических) устройств, подключенных к данному средству вычислительной техники. В то же время на уровне вычислительной сети объекта АС устройствами, как правило, являются

логические понятия. К ним относятся направления и каналы связи, распределенные хранилища данных, группы пользователей (например, «Администратор», «Группа (отдел) разработки приложений» и т.д.), объекты АС в целом;

4) ОС статически маршрутизирует (направляет) потоки данных на уровне отдельного средства вычислительной техники. В то же время на уровне объекта АС, как правило, требуется динамическая маршрутизация между всеми вычислительными средствами объекта, а также между объектами АС в целом с учетом возможности логической привязки пользователей (должностных лиц) к их рабочим местам и перенаправления информационных потоков в зависимости от складывающихся обстоятельств;

5) администрирование вычислительного процесса на уровне ОС ориентировано, прежде всего, на данное СВТ, реже — на группу однородных СВТ, в то время как на уровне объекта АС требуется администрирование приложений всей неоднородной вычислительной сети, состоящей из главных вычислительных модулей, специализированных серверов ЛВС, выделенных рабочих мест (АРМ) и функционирующих в их составе приложений (программ), а также каналов связи с контролем их работоспособности в составе системы.

На рисунке 3 представлена работа узла в доверенном контуре доверенной инфраструктуры.

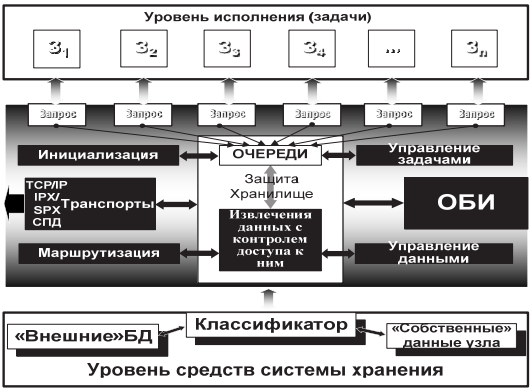

Рис. 3. Организация вычислительного процесса на доверенном узле

Отмеченные противоречия и дополнительные требования к системе защиты обусловливают необходимость дополнения базовых средств защиты информации уровня отдельных ОС некоторыми унифицированными средствами организации вычислительного процесса и управления обработкой информации на уровне объекта АС, инвариантными по от-

ношению к определенным операционным системам и обеспечивающими совместное функционирование "унаследованного", актуального и перспективного программного обеспечения [6].

4. Доверенные элементы распределенной информационной сети. На сегодняшний день основным принципом построения крупных информационных систем является объединение территориально распределенных ЛВС и отдельных компьютеров через сеть Интернет в общую распределенную информационную систему (РИС). Пользователи работают в едином информационном пространстве, разделяемом на зоны с различным набором прав на использование сервисов.

Как правило, используемые программно-аппаратные средства защиты информации разделяются на три категории:

- средства обеспечения доверенной загрузки;
- средства обеспечения доверенности компьютера;
- средства обеспечения защищенного соединения.

Процедуру загрузки, защищенную таким образом, назовем доверенной загрузкой операционной системы.

К средствам обеспечения доверенности компьютера относятся программно-аппаратные комплексы, включающие средства обеспечения доверенной загрузки, СЗИ НСД, средства обеспечения доступа к ресурсам, а также антивирусные средства.

На практике построение защищенных распределенных информационных систем имеет следующие особенности:

- выполнение требований политики ИБ, в частности запуск разрешенных для выполнения задач в рамках изолированной программной среды, необходимо контролировать как для локального, так и для удаленного (подключаемого) сегмента РИС, что не всегда реализуемо на практике;
- для обеспечения конфиденциальности, целостности и доступности данных с возможностью применения ЭЦП необходимо использовать сертифицированные ОС, СЗИ НСД и СКЗИ, а также обеспечить аттестацию рабочих мест пользователей и всей РИС;
- сертифицированные ОС имеют ограничения на установку и обновление компонентов ОС и прикладного ПО и зачастую предоставляют недостаточный функционал;
- стоимость сертифицированных ОС, СЗИ НСД и СКЗИ, а также процедуры аттестации часто превышает стоимость компьютерной техники и прикладного ПО на рабочем месте пользователя.

Таким образом, обеспечить защиту РИС, в частности государственных автоматизированных систем, средствами доверенной вычислительной среды на основе резидентного компонента безопасности в принципе возможно (хотя это требует значительных затрат и связано с рядом

сложностей), но для рабочих мест служащих и персональных компьютеров граждан, которые планируют работать с сервисами государственных автоматизированных систем оказывается слишком сложной.

В настоящее время существует принципиально новая концепция доверенного сеанса связи удаленных пользователей с сервисами доверенной среды РИС через сеть Интернет, развивающая концепцию доверенной вычислительной среды на основе резидентного компонента безопасности. Суть концепции состоит в предоставлении пользователю достаточных условий для защищенной работы с сервисами доверенной РИС на определенный период времени, при выполнении которых не требуется построение изолированной программной среды на компьютере пользователя, но в то же время не снижается класс защищенности РИС.

После выполнения описанных процедур по созданию доверенной среды средствами контроля целостности ОСПО из конфигурационных файлов базовой ОС извлекаются контрольные суммы зарегистрированных приложений и помещаются в специальный раздел (журнал) хранилища данных, доступный (только в режиме просмотра) администратору безопасности. В начале каждого сеанса работы, а также по особому регламенту в процессе работы средства контроля целостности ОСПО обеспечивают проверку наличия доверительной среды. При отрицательном результате производится автоматическая запись о факте нарушения целостности в журнал контроля целостности и завершение работы ядра ОСПО, а также всех зарегистрированных в доверительной среде приложений. Продолжение работы возможно только после восстановления доверенной среды.

Информация, относящаяся к работе ПСЗ ОСПО (пароли, журналы, эталонные значения контрольных сумм и т. д.), должна храниться в специализированном хранилище БД ОСПО и быть недоступной для непосредственного просмотра или модификации. Попытка атаки на уровне базовой ОС неминуемо ведет к нарушению доверенной среды, блокирует работу ядра ПСЗ и как следствие — доступ извне к защищаемой информации [7].

Основной проблемой, с которой сталкиваются специалисты при решении задач построения системы защиты на объектах АС, как указывалось выше, является необходимость перехода к единой и безопасной вычислительной среде, доверенной инфраструктуры в условиях неоднородности программно-аппаратных средств, а также наличия в ряде случаев "унаследованных" систем. При решении этой задачи, как правило, невозможно одновременно полностью отказаться от "старых" платформ. Поэтому необходимо построить всю систему таким образом, чтобы исключить или минимизировать возможность реализации угроз, возникающих из-за использования недоверенных "унаследо-

ванных" платформ.

В доверенной инфраструктуре также должны решаться задачи по защите информации от несанкционированного доступа. Для нейтрализации как явных, так и скрытых угроз в распределенных АС при участии авторов был разработан специальный программно-аппаратный комплекс защиты информации «Ключ-Ш» (далее – СПАК), обеспечивающий построение распределенных АС критической инфраструктуры.

5. Двухуровневое шифрование в доверенной инфраструктуре. Основой функциональной архитектуры СПАК являются подсистемы глобального шифрования и усиленной аутентификации, ориентированные на решение следующих групп задач [8]:

– двухуровневое «прозрачное» шифрование информации на жестких дисках АРМ;

– логическая привязка съемных носителей (Flash, CD, DVD) к заданной группе автономных АРМ за счет «прозрачного» шифрования информации на этих съемных носителях по закрытому ключу;

– использование электронных идентификаторов ruToken для аутентификации пользователей, а также хранения, переноса и резервирования ключевой информации. На рисунке 4 представлена функциональная архитектура доверенной системы шифрования.

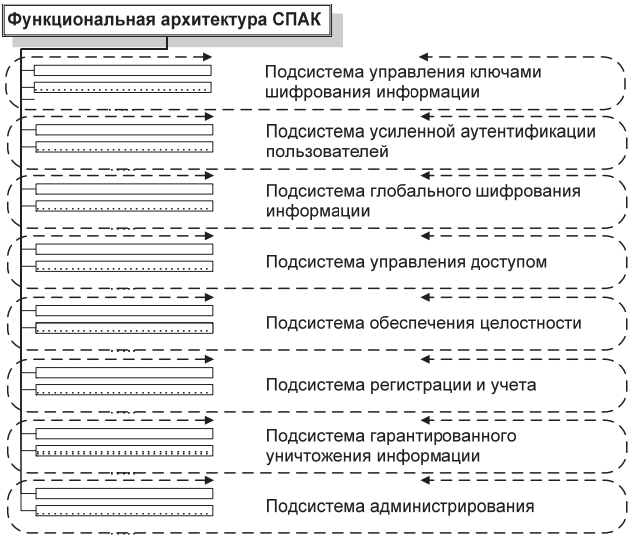

Рис. 4. Функциональная архитектура доверенной системы шифрования

Двухуровневое «прозрачное» шифрование информации на жестких дисках АРМ предполагает наличие двух уровней:

– первый уровень — глобальное шифрование информации по секторам жестких дисков;

– второй уровень — шифрование виртуальных дисков, формируемых на основе информации из файла-контейнера.

Глобальное «прозрачное» шифрование информации в системном разделе жесткого диска АРМ выполняется по закрытому ключу, общему для всех зарегистрированных пользователей. При «прозрачном» шифровании логических и виртуальных дисков предполагается использование индивидуальных ключей.

Для управления «прозрачно» шифруемыми виртуальными дисками предусмотрены такие важные функции, как:

– поддержка возможности переноса файла-контейнера с зашифрованным виртуальным диском с одного защищенного АРМ на другой;

– подключение зашифрованного виртуального диска по сети, в процессе работы с которым передаваемая информация шифруется в режиме реального времени, и по сети передаются только зашифрованные информационные пакеты;

– перенос ключей шифрования виртуальных дисков в аппаратно защищенной памяти электронных идентификаторов ruToken с возможностью доступа к этим ключам только после предъявления соответствующего PIN-кода.

Кроме того, учтена необходимость логической привязки съемных носителей (Flash, CD, DVD) к заданной группе автономных АРМ за счет «прозрачного» шифрования информации на этих съемных носителях по закрытому ключу. Пользователи заданной группы автономных АРМ могут передавать зашифрованные носители для работы с ними с одного АРМ на другой. Вне заданной группы автономных АРМ информация на зашифрованных носителях будет недоступна.

Высокая скорость и стойкость шифрования обеспечивается за счет следующих факторов, положенных в основу построения используемых и запатентованных алгоритмов:

– перенос всех вычислений, требующих больших временных ресурсов, на этап инициализации криптографической подсистемы, который выполняется только в начале сеанса работы пользователя;

– зависимость операций криптографического преобразования не только от рабочих ключей, но и от преобразуемых данных и промежуточных результатов преобразования, что повышает степень псевдослучайности в алгоритме непосредственных преобразований;

– снижение сложности алгоритма непосредственных криптографических преобразований за счет повышения его стойкости.

Для фиксированного уровня стойкости используемые алгоритмы обеспечивают более низкую сложность алгоритмов непосредственного криптографического преобразования информации. За счет этого достигается более высокая скорость шифрования.

Для аппаратной поддержки процесса аутентификации и хранения ключей шифрования в составе СПАК используется сертифицированный электронный идентификатор ruToken, закрепляемый за каждым пользователем.

При формировании архитектуры СПАК изначально учитывались основы реализации технологических схем защищенной автоматизированной обработки информации:

– управление ключами шифрования на основе инфраструктуры открытых ключей;

– обеспечение подлинности электронных документов за счет формирования и проверки их электронных подписей;

– обеспечение конфиденциальности электронных документов за счет их шифрования.

Построение подсистемы управления ключами шифрования выполнялось исходя из следующих требований:

– должна быть обеспечена гибкость распределения ключей шифрования информации;

– подсистема управления ключами не должна требовать доверия взаимодействующих друг с другом сторон;

– скорость криптографических преобразований должна обеспечивать шифрование информации в режиме реального времени.

Реализация первых двух требований выполнена за счет асимметричного принципа построения ключей верхнего уровня, а реализация третьего требования – за счет использования ключей скоростного симметричного шифрования.

В подсистеме управления ключами шифрования СПАК используются следующие базовые уровни ключей:

– первичные пары асимметричных ключей (первичные ключи), включая личные ключи пользователей, формируемые в соответствии с российским стандартом цифровой подписи ГОСТ Р 34.10 и используемые для распределения ключей, а также выработки на основе цифровой подписи вторичных ключей симметричного шифрования;

– вторичные ключи симметричного шифрования (вторичные ключи), формируемые по алгоритму Диффи–Хеллмана на основе первичных пар асимметричных ключей, и используемые для шифрования носителей информации и информационного трафика;

– ключи доступа, используемые для защиты первичных ключей, связок ключей пользователя, а также базы данных СПАК.

Первый уровень ключей специального преобразования информации за счет асимметричного принципа построения обеспечивает гибкость распределения ключей и не требует доверия взаимодействующих друг с другом сторон.

Второй уровень ключей специального преобразования информации за счет симметричного принципа построения и использования скоростных алгоритмов криптографических преобразований обеспечивает шифрование информации в режиме реального времени.

Третий уровень ключей специального преобразования информации за счет многоуровневого шифрования обеспечивает надежную защиту ключей первых двух уровней.

Для каждого пользователя в СПАК по ГОСТ 34.10 генерируется личная пара асимметричных ключей, которая хранится в профиле пользователя в базе данных (БД) системы защиты. Закрытый ключ этой пары ключей зашифрован по ключу, генерируемому по специальному алгоритму (алгоритму SSE2) на основе пароля (PIN-кода) этого пользователя. Вводимый пароль (PIN-код) пользователя используется для расшифрования закрытого ключа личной пары асимметричных ключей. Открытый ключ личной пары асимметричных ключей подписан по закрытому первичному ключу АРМ.

Аутентификация пользователей в СПАК основана на использовании цифровой подписи. Для аутентификации пользователя модуль управления БД СПАК направляет агенту аутентификации запрос на цифровую подпись сгенерированного случайного числа, формируемую на основе личного закрытого ключа этого пользователя. Если пароль (PIN-код) был введен пользователем неправильно, то агент аутентификации не сможет правильно расшифровать личный закрытый ключ пользователя, а, следовательно, не сможет создать требуемую подпись. В противном случае проверка цифровой подписи даст положительный результат, и пользователь сможет продолжить работу. В случае положительной аутентификации пользователя система защиты обеспечивает доступ со стороны пользователя к защищенным информационным ресурсам АРМ в соответствии со схемой использования ключей при доступе к зашифрованным объектам.

Предполагается, что предварительно соответствующие зашифрованные информационные объекты должны быть созданы. Для создания зашифрованного информационного объекта генерируется первичная пара асимметричных ключей (по ГОСТ 34.10), которая закрепляется за данным объектом. В базе данных ПАК для каждой первич-

ной и личной пары асимметричных ключей используются следующие атрибуты:

– числовой идентификатор ключевой пары, а также дата и время ее создания;

– числовой идентификатор пользователя, создавшего ключевую пару;

– имя (символьный идентификатор) ключевой пары;

– идентификатор алгоритма шифрования объекта, для которого создана ключевая пара;

– описание ключевой пары;

– открытый и закрытый ключи.

Защищаемый объект шифруется по вторичному ключу симметричного шифрования, формируемому по алгоритму Диффи–Хеллмана на основе соответствующей объекту первичной пары асимметричных ключей. Первичная пара асимметричных ключей, закрепленная за объектом, защищается с помощью ключей доступа.

Система управления цифровыми сертификатами открытых ключей реализуется на основе использования удостоверяющего центра. В соответствии с международным признанным форматом для определения сертификатов открытых ключей (стандартом X.509 ITU), выдаваемый пользователю цифровой сертификат включает следующие элементы:

– версия, серийный номер и срок действия сертификата;

– информация о доверителе, выдавшем сертификата;

– информация о владельце сертификата (имя и фамилия, идентификатор, организация, адрес и др.);

– открытый ключ владельца сертификата;

– тип используемого алгоритма цифровой подписи;

– цифровая подпись всего содержимого сертификата, сформированная выдавшим сертификат удостоверяющим центром.

Ответственность за подлинность указанной в сертификате информации несет удостоверяющий центр, выдавший сертификат и сформировавший под ним свою подпись. Основными компонентами удостоверяющего центра являются центры сертификации, регистрации и сетевой справочник сертификатов [9]. На рисунке 5 показан пример использования ключей при доступе к зашифрованному объекту доверенной инфраструктуры.

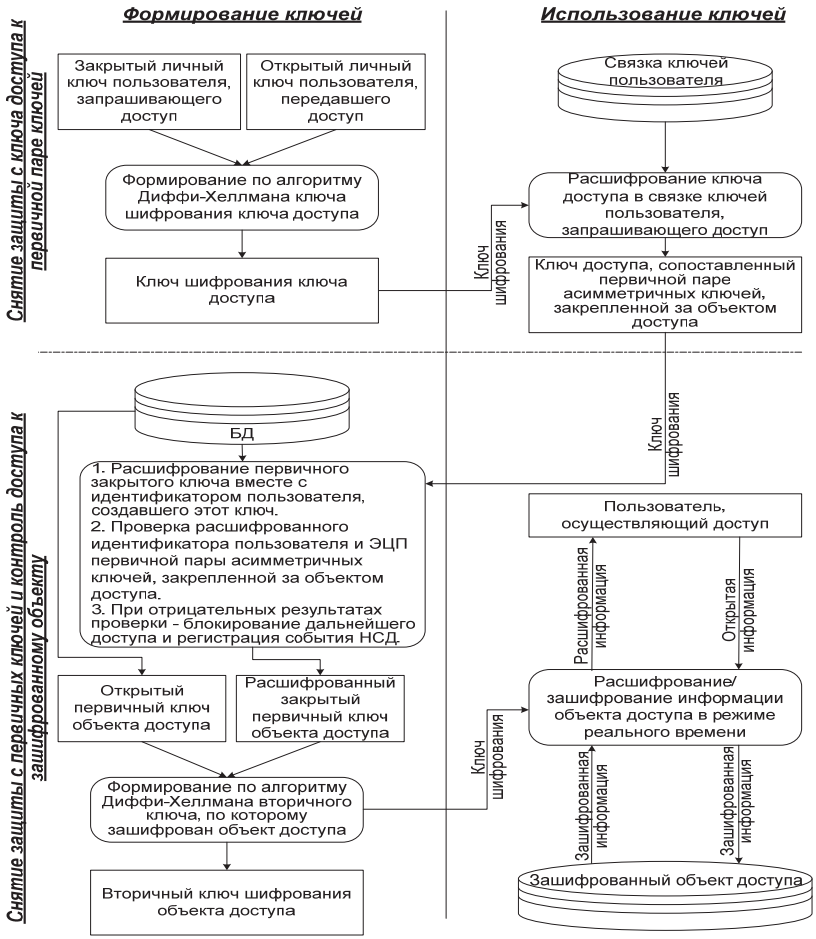

Рис. 5. Схема использования ключей при доступе к зашифрованному объекту

Центр сертификации обеспечивает формирование цифровых сертификатов. Кроме цифровых сертификатов, планируемых для использования, Центр сертификации формирует список отозванных сертификатов.

Центр регистрации предназначен для регистрации конечных пользователей. Основная задача Центра регистрации — регистрация пользователей и обеспечение их взаимодействия с Центром сертификации. В задачи Центра регистрации также входит публикация сертификатов и списка отозванных сертификатов в сетевом справочнике.

Центр регистрации является единственной точкой входа и регистрации пользователей. В качестве операционной платформы СПАК вследствие объективных причин предложено использование комбинированной операционной среды:

– для защищенного выполнения прикладных процессов и целевых функций АС – ОС Windows;

– для критичных функций настройки режимов защиты, управления ключами и конфигурирования криптомодулей — аналог ядра доверенной ОС Linux, реализованный как программный эмулятор аппаратного модуля доверенной загрузки.

СПАК основан на формальной и верифицированной модели управления доступом к защищаемым ресурсам АС. Показано, что разграничение доступа к информационным ресурсам (файлам, каталогам, томам NTFS, отчуждаемым носителям, портам ввода-вывода и принтерам) происходит в первую очередь согласно мандатному принципу контроля доступа, а дискреционные правила контроля доступа действуют только в пределах разрешений, установленных в соответствии с мандатным принципом. Эффективный доступ субъекта к информационным ресурсам определяется как результат пересечения атрибутов мандатного и дискреционного доступа. Представлены уровни, реализуемые в СПАК для защиты от обхода диспетчера доступа.

Таким образом, при разработке СПАК «Ключ-Ш» реализована технология построения комплексной системы информационно-компьютерной безопасности с учетом информационных рисков, основанная на учете всех исходных требований, существующих угроз и влияющих на безопасность факторов при комплексном использовании наиболее эффективных мер, методов и средств защиты. Применение СПАК «Ключ-Ш» в АС доверенной инфраструктуры позволяет снизить показатели информационных рисков до приемлемого уровня, при котором обеспечивается гарантированная степень защищенности распределенных АС.

6. Организация защиты контура в доверенной инфраструктуре. К средствам защиты неоднородной АС относятся, прежде всего, средства защиты "периметра" - межсетевые экраны (МЭ), антивирусной защиты, разграничения доступа, закрытия канала связи - связанные с защитой от "внешних атак". Хотя возможность "внешней угрозы" несколько преувеличена, она реальна. Основным "нарушителем" для любой АС является авторизованный пользователь с высоким статусом. Поэтому система безопасности должна строиться с учетом фактора "внутреннего нарушителя", как самого опасного субъекта. Напомним, что большинство удачных "внешних атак" было проведено с использованием внутреннего ресурса системы. Поэтому в АС необходимо предусмотреть механизмы, позволяющие строго регламентировать доступ к внутренним ресурсам системы на базе "ролевых сцена-

риев", должностных инструкций, ведения журналов безопасности и системных событий для предотвращения и выявления источников "внутренних атак". Здесь же важной является задача шифрования (закрытия) канала обмена между любыми абонентами АС. Это опять-таки задача СЗИ ОСПО. Если существует тесная связь между СЗИ на "периметре", антивирусного пакета и пр., то система безопасности будет работать непротиворечиво и прозрачно для пользователя, что является немаловажным фактором, влияющим в конечном итоге на работоспособность системы в целом. Самые общие задачи системы защиты информации ОСПО таковы:

- организация безопасного доступа объектов АС в каналы связи, в том числе открытые;
- построение единой политики безопасности в рамках гетерогенной распределенной сети АС;
- защита от НСД к информации, принимаемой, обрабатываемой, передаваемой и хранимой в АС по необходимому классу защищенности, в том числе - до сведений, содержащих государственную тайну, на выделенных локальных узлах АС;
- передача меток конфиденциальности в пределах защищенной наложенной сети АС, реализованной средствами ОСПО;
- осуществление защитных мер (в том числе организационных) по закрытию каналов передачи данных, а также возможных каналов утечки информации.

МЭ должен представлять собой программный комплекс, управляемый специально разработанной операционной системой. Одной из особенностей МЭ должна являться простота его установки, исчерпывающий набор настроек по умолчанию, которые позволяют системному администратору быстро организовать доступ в Интернет, решая одновременно проблему острой нехватки квалифицированного персонала на местах. Серверная часть является точкой доступа, обеспечивает безопасное и надежное, экономически оправданное взаимодействие с Сетью, генерацию собственной внутренней сети Интранет посредством полного и понятного механизма маршрутизации IP-пакетов с функциями фильтрации, механизма трансляции адресов (NAT) и прокси-фильтрами сетевого уровня по протоколам HTTP, HTTPS и FTP. Поэтому основными функциями МЭ являются:

- обслуживание локальных узлов АС и защиты их от попыток несанкционированного доступа (НСД);
- обеспечение возможности создания централизованной ведомственной АС на основе локальных сетей, оснащенных МЭ, и связанных через глобальную сеть Интернет;
- разграничение доступа к ресурсам и сервисам на основе заданных правил;

- обеспечения возможности сквозного контроля и управления состоянием АС;

- обеспечение возможности поддержания актуального состояния прикладного ПО АС посредством локальной и удаленной установки ПО;

- обеспечения возможности реализации единой политики безопасности АС [10].

Таким образом, МЭ должен отвечать всем необходимым требованиям, предъявляемым к межсетевым экранам как к средствам защиты периметра АС, а именно:

- контроль доступа с поддержкой динамической адресации;
- трансляция сетевых адресов;
- зависимость требований безопасности от интерфейса МЭ;
- подсчет трафика и генерация отчетов;
- удобство и простота управления МЭ авторизованным Администратором;
- интеграция с другими средствами защиты информации;
- "прозрачное" функционирование без потери производительности сети;
- обеспечение технической поддержки.

На рисунке 6 представлена схема применения доверенного МЭ – контура при выходе в сеть Интернет из доверенной инфраструктуры.

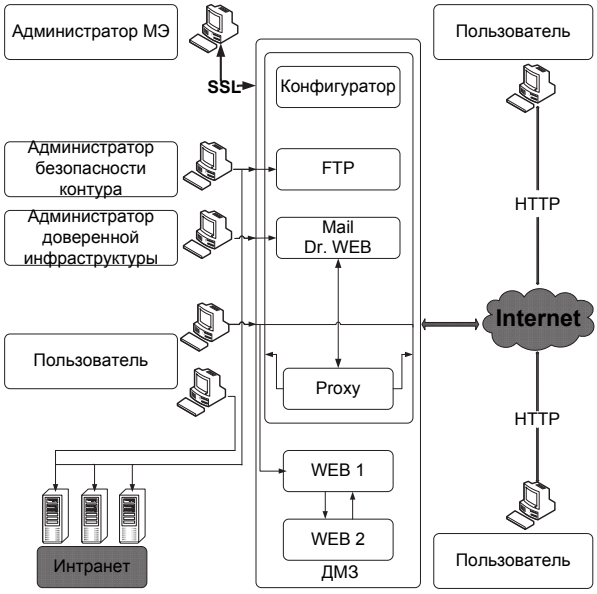

Рис. 6. Защита обработки данных в доверенном контуре

7. Заключение. Рассмотренный в статье подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры позволяет построить политику администрирования безопасности в распределенной системе на различных платформах. Под управлением администратора доверенной инфраструктуры будет производиться контроль всех действий в системе, включая фискальный. Применение перечисленных способов организации защиты информации в гетерогенных вычислительных сетях дает следующие преимущества:

1) пользователю предоставляется необходимый функционал и достаточный уровень защиты (близкий к уровню доверенного компьютера с набором сертифицированных ОС, СЗИ НСД и СКЗИ);

2) стоимость средств обеспечения доверенного сеанса значительно ниже стоимости оборудования рабочего места необходимого для реализации политики изолированной программной среды набором СЗИ;

3) клиент доверенного сеанса связи является мобильным загрузочным устройством, готовым к работе на любом недоверенном компьютере;

4) средства обеспечения доверенного сеанса не накладывают ограничений на работу пользователя с компьютером вне доверенного сеанса связи;

5) применение «Ключ-Ш» в АС позволяет снизить показатели информационных рисков до приемлемого уровня, при котором обеспечивается гарантированная степень защищенности распределенных АС.

Литература

1. *Ручкин В.Н., Фулин В.А.* Архитектура компьютерных сетей // Диалог-МИФИ. 2008. 76 с.
2. *Андерсон К., Минаси М.* Локальные сети. Полное руководство // СПб.: КОРОНА принт. 1999. 458 с.
3. *Косарев В.П., Еремин Л.В.* Компьютерные системы и сети // Финансы и статистика. 1999. С .260–281.
4. *Новиков С.В., Зима В.М., Андрушкевич Д.В.* Организация защиты информации в гетерогенных вычислительных сетях // Информационно-методический журнал «Инсайд». СПб.: ИД Афина. 2014. № 3. С. 21–28.
5. *Кульгин М.В.* Технология корпоративных сетей. Энциклопедия // СПб.: Питер. 2001. 699 с.
6. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов // СПб.: Питер. 2009. 352 с
7. *Суворов А.Б.* Телекоммуникационные системы, компьютерные сети и Интернет // СПб.: Феникс. 2010. 383 с.
8. *Зима В.М., Клюев А.В., Литвинов О.А., Ломако А.Г., Петров А.Т.* Основы защиты информации от несанкционированного доступа в автоматизированных сис-

темах конфиденциального делопроизводства // Труды СПИИРАН. Вып. 3. Т. 2. 2006. С. 84–95.
9. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Компьютерные сети и защита передаваемой информации // СПб.: издательство СПбГУ. 1998. 328 с.
10. *Здирук К.Б.* Вопросы организации защищенной системы хранения и обработки данных в гетерогенных вычислительных сетях // Вопросы защиты информации. Журнал. М.: 2007. С. 46–52.

References

1. Ruchkin V.N., Fulin V.A. *Arhitektura komp'juternyh setej* [Architecture of computer networks]. Dialog-MIFI. 2008. 76 p. (In Russ.).
2. Anderson K., Minasi M. *Lokal'nye seti. Polnoe rukovodstvo* [LAN. Full guide]. SPb.: KORONA print. 1999. 458 p. (In Russ.).
3. Kosarev V.P., Eremin L.V. [Computer systems and networks]. *Finansy i statistika – Finance and statistics.* 1999. pp.260–281. (In Russ.).
4. Novikov S. V., Zima V. M., Andrushkevich D. V. [Organization of information security in heterogeneous computer networks]. *Informacionno-metodicheskij zhurnal "Insajd" – Information-methodical journal "Inside".* SPb.: ID Afina. 2014. vol. 3. pp. 21–28. (In Russ.).
5. Kuligin M.V. *Tehnologija korporativnyh setej. Jenciklopedija* [Technology enterprise networks. Encyclopedia]. SPb.: Piter. 2001. 699 p. (In Russ.).
6. Olifer V. G., Olifer N.A. *Komp'juternye seti. Principy, tehnologii, protokoly. Uchebnik dlja vuzov* [Computer network. Principles, technologies and protocols. Textbook for high schools]. SPb.: Peter. 2009. 352 p. (In Russ.).
7. Suvorov A. B. *Telekommunikacionnye sistemy, komp'juternye seti i Internet* [Telecommunication systems, computer networks and Internet]. SPb.: Feniks. 2010. 383 p. (In Russ.).
8. Zima V.M., Klyuyev A.V., Litvinov O.A., Lomako A.G., Petrov A.T. [Framework for the protection of information from unauthorized access automated systems confidential records management]. *Trudy SPIIRAN – SPIIRAS Proceeding.* 2006. vol. 3. issue 2. pp. 84–95. (In Russ.).
9. Zima V.M., Moldovyan A.A., Moldovyan N.A. *Komp'juternye seti i zashhita peredavaemoj informacii* [Computer networks and the protection of information transmitted]. SPb.: izdatel'stvo SPbGU. 1998. 328 p. (In Russ.).
10. Zdiruk K. B. [Organization protected storage system and data processing in heterogeneous computer networks]. *Voprosy zashhity informacii. Zhurnal – The issues of information security. Journal*. M.: 2007. pp. 46–52. (In Russ.).

Новиков Сергей Витальевич — к-т воен. наук, доцент кафедры систем сбора и обработки информации Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации в автоматизированных системах специального назначения, представление обстановки на электронной карте ГИС, информационная безопасность. Число научных публикаций — 24. novikov1976@mail.ru; Ждановская улица д. 13, г. Санкт-Петербург, 197198, РФ; р.т. 7(812)347-9687.

Novikov Sergey Vitalyevich — Ph.D., associate professor of system for collecting and processing information department Mozhaisky military space Academy. Research interests: information security in automated systems for special purposes, the representation of the situation on the electronic map, GIS, information security. The number of publications — 24. novikov1976@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone 7(812)347-9687.

Зима Владимир Михайлович — к-т техн. наук, профессор кафедры систем сбора и обработки данных Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации в информационных сетях, автоматизированных системах. Число научных публикаций —105. vladimir_zima@mail.ru; улица Ждановкая д. 13, г. Санкт-Петербург, 197198, РФ; р.т. +7(812)347-9687.

Zima Vladimir Mikhailovich — Ph.D., associate professor, professor of system for collecting and processing information department Mozhaisky military space Academy. Research interests: information security in data networks, automated systems. The number of publications — 105. vladimir_zima@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone +7(812)347-9687.

Андрушкевич Дарья Владимировна — адъюнкт кафедры систем сбора и обработки информации Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации в информационных сетях, автоматизированных системах. Число научных публикаций — 8. andrushkevich.d@mail.ru; улица Ждановская д. 13, г. Санкт-Петербург, 197198, РФ; р.т. +7(812)347-9687.

Andrushkevich Daria Vladimirovna — Ph.D. student of system for collecting and processing information department Mozhaisky military space Academy. Research interests: information security in data networks, automated systems. The number of publications — 8. andrushkevich.d@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone +7(812)347-9687.

РЕФЕРАТ

Новиков С.В., Зима В.М., Андрушкевич Д.В. **Подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры.**

В статье предлагается подход к построению распределенных вычислительных сетей и организации защиты информации с использованием доверенной инфраструктуры.

Приводится инфраструктура, которая будет состоять из контура, в состав которого будут входить: доверенный контроль, доверенный канал связи, доверенные сегменты распределенной сети, доверенные АРМ с различными платформами ОС, доверенное специальное программное обеспечение с НДВ, доверенная система шифрования, доверенные администраторы всех сегментов сети, администратор доверенной инфраструктуры.

Для организации защиты информации на различных узлах распределенных сетей обработки данных предлагается введение данного контура с администраторским управлением на каждом сегменте контура под управлением администратора доверенной инфраструктуры.

В данной статье анализируются некоторые из подходов защиты сегментов доверенной инфраструктуры, а именно: организация защиты информации в доверенном контуре на различных платформах ОС; доверенные элементы распределенной информационной системы; двухуровневое шифрование в доверенной инфраструктуре; доверенный контур в доверенной инфраструктуре, как защита периметра.

Результаты работы показывают, что подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры позволяет построить политику администрирования безопасности в распределенной системе на различных платформах. Под управлением администратора доверенной инфраструктуры будет производиться контроль всех действий в системе, включая фискальный.

SUMMARY

Novikov S.V., Zima V.M., Andrushkevich D.V. **Approach to Building Secure Distributed Networks of Data Processing based on Trusted Infrastructure.**

In article approach to creation of the distributed computer networks and the organization of information security with use of the entrusted infrastructure is offered.

The infrastructure, which will consist of the entrusted control, the entrusted communication channel, the entrusted segments of the distributed network entrusted an automated workplace with the OS various platforms, the entrusted special software with NDV, the entrusted system of enciphering, the entrusted administrators of all segments of a network, the administrator of the entrusted infrastructure, is presented.

For the organization of information security on various knots of the distributed networks of data processing introduction of the contour with administrator management on each segment of a contour under control of the administrator of the entrusted infrastructure is offered.

In this article some of approaches of protection of segments of the entrusted infrastructure, are analyzed namely: the organization of information security in the entrusted contour on the OS various platforms; the entrusted elements of the distributed information system; two-level enciphering in the entrusted infrastructure; the entrusted contour in the entrusted infrastructure, as defense of perimeter.

Results of work show that approach to creation of the protected distributed data processing networks on the basis of the entrusted infrastructure allows to construct policy of administration of safety in the distributed system on various platforms. Under control of the administrator of the entrusted infrastructure control of all actions in system, including the fiscal will be made.