АВТОМАТИЗИРОВАННАЯСИСТЕМА ДЛЯ РАБОТЫ С ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО ДОПУСКА НА БАЗЕ ТОНКИХ КЛИЕНТОВ (ТЕРМИНАЛЬНЫЙ РЕЖИМ) С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

С. А. Якунина, Н. Н. Вовк, А. Н. Гаврилин, А. С. Егоров, Р. В. Ефремов, Е. А. Жуненко, К. В. Леванов, И. В. Понеделко

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90).

Тонкий клиент (англ. Thin client) в компьютерных технологиях – компьютер в сетях с терминальной архитектурой, который переносит всю или большую часть задач по обработке информации на сервер (рис.1). Тонкий клиент не имеет жесткого диска, использует специализированную локальную операционную систему, одна из задач которой организовать сессию с терминальным сервером для работы пользователя.

Рис. 1. Модель использования тонких клиентов в сетях с терминальной архитектурой

Технология «тонкий клиент» подразумевает централизованную архитектуру с центральным сервером приложений, который может быть связан с сервером баз данных, также с резервным терминальным сервером для повышения отказоустойчивости и надежности системы и с подключенными к нему компьютерами – терминалами.

В общем случае тонкие клиенты представляют собой персональные электронные устройства, обеспечивающие доступ к терминальной среде (Server-Based Computing – SBC) или к виртуальной среде рабочих мест (Virtual Desktop Infrastructure – VDI). Их появление и развитие обусловлено общей парадигмой эволюции информационных технологий для делового применения в стремлении сократить затраты на автоматизацию делопроизводства. Есть широко известный термин совокупная стоимость владения (Total Costof Ownership – TCO) для любого рабочего инструмента, так вот основное интегральное преимущество тонких клиентов – это снижение показателя TCO в сравнении с использованием традиционных персональных компьютеров и как итоговый результат снижение себестоимости любого конечного продукта. Если конкретизировать, то снижение TCO для тонкого клиента складывается из снижения затрат на развертывание, эксплуатацию и управление, также можно отметить более длительный жизненный цикл и повышение безопасности [1].

В качестве операционной системы, устанавливаемой на сервере для использования на всех тонких клиентах, подключенных к данному серверу, предлагаем использовать операционную систему специального назначения «Astra Linux Special Edition» (далее – ОС СН).). ОС СН предназначена для создания на её основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию до грифа «совершенно секретно» включительно [2].

Данная ОС СН является операционной системой типа «А» и соответствует требованиям документов «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016) и «Профиль защиты операционных систем типа «А» второго класса защиты. ИТ.ОС.А2.ПЗ» (ФСТЭК России, 2016) (рис. 2).

ОС СН является Российской разработкой и первой прошла сертификацию по новым требованиям ФСТЭК России. Благодаря новым требованиям, применение в государственных информационных системах операционных систем, исходные коды которых (в частности, систем безопасности) не представлены для проверки, существенно осложнено.

Рис. 2. Функции средств защиты информации от несанкционированного доступа ОС СН

Программно-аппаратный комплекс

При разработке данного проекта были учтены требования безопасности к организации автоматизированного рабочего места для работы с информацией ограниченного допуска. Комплекс разработан на базе технологии «тонкий клиент» (терминальный режим) с использованием ОС СН «Astra Linux Special Edition».

Комплекс позволяет реализовать следующие требования безопасности информации.

- Мандатное разграничение доступа

В операционной системе реализован механизм мандатного разграничения доступа – разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как принудительный контроль доступа. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

Согласно требованиям ФСТЭК мандатное управление доступом или «метки доступа» являются ключевым отличием систем защиты государственной тайны РФ старших классов защитных систем на классическом разделении прав по матрице доступа.

Пример: субъект «Пользователь № 2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющему метку «для служебного пользования». В то же время, субъект «Пользователь № 1» с допуском уровня «секретно» право доступа к объекту с меткой «для служебного пользования» имеет.

При этом принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение / запись / исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом. Для удобства работы пользователей и разработки прикладных программ, разработана системная библиотека с удобным программным интерфейсом доступа к механизму мандатного разграничения доступа. Обеспечено взаимодействие входящих в состав операционной системы клиент-серверных компонент, а также файловых систем(ext3, CIFS) с механизмом мандатного разграничения доступа.

- Изоляция модулей

Ядро операционной системы обеспечивает для каждого процесса в системе собственное изолированное адресное пространство. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический. Любой доступ нескольких процессов к одному и тому же участку памяти обрабатывается диспетчером доступа в соответствии с дискреционными и мандатными правилами разграничения доступа.

- Очистка оперативной и внешней памяти и гарантированное удаление файлов

Операционная система выполняет очистку неиспользуемых блоков файловой системы непосредственно при их освобождении. Работа этой подсистемы снижает скорость выполнения операций удаления и усечения размера файла, однако возможна настройка данной подсистемы для обеспечения работы

файловых систем с различными показателями производительности.

- Маркировка документов

Разработанный механизм маркировки позволяет серверу печати (CUPS) проставлять необходимые учетные данные в выводимых на печать документах. Мандатные атрибуты автоматически связываются с заданием для печати на основе мандатного контекста получаемого сетевого соединения. Вывод на печать документов без маркировки субъектами доступа, работающими в мандатном контексте с грифом выше «несекретно», невозможен.

- Регистрация событий

Реализована оригинальная подсистема протоколирования, интегрированная во все компоненты операционной системы и осуществляющая надёжную регистрацию событий с использованием специального сервиса.

- Режим ограничения действий пользователя (режим «киоск»)

Режим «киоск» служит для ограничения прав пользователей в системе. Степень этих ограничений задается маской киоска, которая накладывается на права доступа к файлу при любой попытке пользователя получить доступ. Для установки прав доступа существует система профилей - файлы с готовыми наборами прав доступа для запуска каких-либо программ. Также есть средства создания таких профилей под любые пользовательские задачи. При входе пользователя в систему права доступа из конфигурационного файла устанавливаются автоматически.

- Защита адресного пространства процессов

В операционной системе для исполняемых файлов используется формат, позволяющий установить режим доступа к сегментам в адресном пространстве процесса. Централизованная система сборки программного обеспечения гарантирует установку минимального режима, необходимого для функционирования программного обеспечения. Также существует возможность использования технологии NOT EXECUTE BIT, поддерживаемой современными процессорами.

- Механизм контроля замкнутости программной среды

Реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов в формате ELF. Проверка производится на основе проверки векторов аутентичности, рассчитанных в соответствии с ГОСТ Р 34.10-2001 и внедряемых в исполняемые файлы в процессе сборки. Предусмотрена возможность предоставления сторонним разработчикам программного средства для внедрения векторов аутентичности в разрабатываемое ими программное обеспечение.

- Контроль целостности

Для решения задач контроля целостности применяется функция хэширования в соответствии с ГОСТ Р 34.11-94. Базовой утилитой контроля целостности является программное средство на основе открытого проекта «Another File Integrity Checker».

- Средства организации домена

Для организации доменной структуры разработана подсистема Astra Linux Directory (ALD) на базе открытых стандартов LDAP. Эта подсистема предоставляет средства для организации домена и единого пространства пользователей, которые обеспечивают:

– сквозную аутентификацию в сети;

– централизацию хранения информации об окружении пользователей;

– централизацию хранения настроек системы защиты информации на сервере;

– централизацию управления серверами DNS и DHCP;

– интеграцию в домен защищенных серверов СУБД, серверов печати, электронной почты, web-сервисов и др.;

– централизованный аудит событий безопасности в рамках домена.

- Защищенная реляционная СУБД

В состав операционной системы входит объектно-реляционная СУБД PostgreSQL, в которой реализованы дискреционный и мандатный механизмы контроля доступа к защищаемым ресурсам БД. В основе мандатного механизма разграничения доступа лежит управление доступом к защищаемым ресурсам БД на основе иерархических и неиерархических меток доступа. Это позволяет реализовать многоуровневую защиту с обеспечением разграничения доступа пользователей к защищаемым ресурсам БД и управление потоками информации. В качестве иерархических и неиерархических меток доступа при использовании СУБД используются метки конфиденциальности или метки безопасности операционной системы. Проведены необходимые работы по интеграции СУБД с подсистемой аудита и средствами организации домена.

- Защищенный комплекс программ гипертекстовой обработки данных

В состав защищенного комплекса программ гипертекстовой обработки данных входят браузер Mozilla Firefox и web-сервер Apache, интегрированный со встроенными средствами защиты информации для обеспечения мандатного разграничения доступа при организации удаленного доступа к информационным ресурсам.

Благодаря использованию архитектуры аппаратных средств – тонкий клиент (терминальный доступ), повышается безопасность корпоративных данных. Тонкие клиенты не имеют каких-либо устройств для хранения и записи информации пользователем. Абсолютно вся информация хранится на сервере и не передается по сети, снижается риск хищения данных и атаки вирусов. Для обеспечения повышенной безопасности можно воспользоваться дополнительными средствами, например, устройством чтения смарт-карт, usb-ключом или биометрическим считывателем отпечатков пальцев, которые подключаются к терминалу и предоставляют более высокий и сложный уровень аутентификации пользователей.

Преимущества тонких клиентов

Непосредственно на пользовательских терминалах (рис. 3) отсутствует возможность хранения конфиденциальных данных; нет съемных накопителей; на терминальном сервере можно обеспечить защиту от копирования важной информации на внешние носители на рабочих местах. Все данные хранятся на серверах, где регулярно и централизованно резервируются. Установка нового и обновление существующего программного обеспечения происходит значительно быстрее и проще. Наличие «контролируемой» среды на терминалах не позволяет пользователям запускать неразрешенные администраторами приложения.

Тонкие клиенты служат дольше и реже ломаются. Отсутствует шум, так как в них нет движущихся частей. Обеспечивается более продолжительный срок соответствия корпоративному стандарту – нормативный срок службы персонального компьютера составляет пять-семь лет, а если их меняют вследствие поломок или модернизации через два-три года, то возникает риск создания «зоопарка» оборудования. Терминалы морально не устаревают – рост требований к программному обеспечению вызывает лишь необходимость модернизации ядра терминальной системы, то есть сервера (рис. 4).

Рис. 3. Внешний вид тонкого клиента

Рис. 4. Внешний вид сервера тонкого клиента

Преимущества технологии «тонкий клиент»:

- снижение начальных затрат на приобретение оборудования, вследствие минимальных требований к конфигурации;
- снижение энергопотребления в несколько раз;
- унификация (одинаковый набор ПО для всех пользователей);
- простота администрирования (нет необходимости настраивать каждый компьютер по отдельности);
- экономия времени системного администратора. Все тонкие клиенты абсолютно одинаковы, вероятность поломок сведена к минимуму, а программное обеспечение установлено только на сервере;
- масштабируемость, созданный единожды образ системы для работы всей группы пользователей позволяет при минимальных затратах поддерживать легко масштабируемую сеть. Возможно быстрое создание любого количества новых рабочих мест;
- безопасность и отказоустойчивость. Терминал, загружаясь, получает операционную систему «от производителя», настройка которой осуществляется только отделом информационной поддержки. Все модификации операционной системы и прикладных программ никак не влияют ни на других пользователей, ни на образ, хранящийся на сервере. Вся пользовательская информация хранится на сервере и регулярно резервируется, что увеличивает отказоустойчивость;
- защита от утечек информации (нет локальных носителей – нет возможности делать копии документов на съемные носители информации);
- высокое быстродействие, по сравнению с отдельными рабочими станциями;
- простота наращивания вычислительной мощности (сервер легче модернизировать, чем весь парк компьютеров);
- ускорение работы корпоративных систем;
- повышенная эргономика.

Экономическая выгода использования тонких клиентов

Тонкие клиенты позволяют существенно экономить не только при первичном приобретении, но и при последующем их использовании за счет высокой отказоустойчивости, меньшему потреблению электроэнергию.

По оценке Gartner* при использовании тонких клиентов совокупная стоимость владения (Total Costof Ownership, TCO) сокращается до 40 % по сравнению со стационарным ПК или ноутбуком. Причем TCO состоит из ряда показателей затрат,

* исследовательская и консалтинговая компания, специализирующаяся на рынках информационных технологий. Наиболее известна введением в употребление таких терминов (ERP, магический квадрант, цикл зрелости технологий), а также регулярными исследованиями рынков информационных технологий и аппаратного обеспечения

включая расходы на первичное приобретение оборудования, на последующее его обслуживание и модернизацию. При этом сокращение расходов в процессе эксплуатации нужно учитывать в первую очередь, поскольку согласно оценке Gartner затраты на приобретение составляют лишь четверть от общих затрат на последующую эксплуатацию этого же оборудования. Также на снижение ТСО влияет более низкая вероятность сбоев тонких клиентов (рис. 5).

Экономические и эксплуатационные преимущества использования тонких клиентов:

- экономия при первичном приобретении. Тонкие клиенты требуют более низких первоначальных затрат на приобретение. По сравнению с обычным ПК стоимость тонкого клиента в среднем на 20 % ниже;
- экономия на программном обеспечении. Также существенно экономятся расходы на покупку программного обеспечения, т.к. тонкий клиент не требует локальной операционной системы, средств антивирусной защиты и других пользовательских приложений;
- сокращение затрат на последующее обслуживание и модернизацию пользовательских рабочих мест. Время наработки на отказ (Mean time between failures, MTBF) для тонких клиентов составляет 100 тысяч часов. При этом для стационарных ПК данный показатель варьируется в пределах 20–30 тысяч часов;
- сокращение затрат на электроэнергию. Тонкий клиент в среднем потребляет в 50 раз меньше электроэнергии, чем стационарный ПК с усредненными характеристиками;
- повышение эргономичности. Тонкие клиенты работают практически бесшумно, имеют небольшие размеры и не занимают много места в офисном пространстве. Тонкий клиент занимает в среднем в 4 раза меньше места, чем обычный ПК.

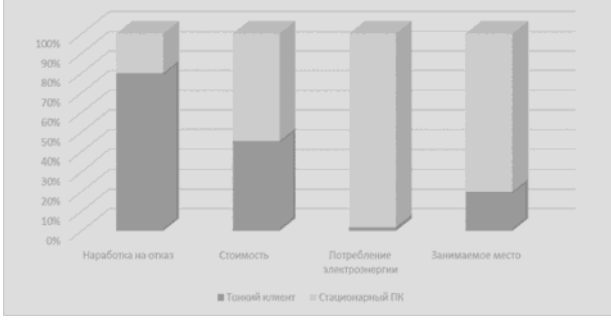

Рис. 5. Сравнение соотношений показателей для тонкого клиента и стационарного ПК

Типовой проект автоматизированной системы

Существует отработанный процесс создания автоматизированных систем, основанных на терминальной архитектуре работы с данными в корпорациях, не связанных с предприятиями стратегического назначения.

С развитием технологий по защите информации от несанкционированного доступа в отечественном кластере и развитием технологий шифрования и скоростной передачи данных от терминала к серверу появилась возможность интегрировать опыт терминализации ИТ инфраструктуры, полученный в корпорациях гражданской направленности, в инфраструктуру цифрового документооборота предприятия стратегического значения.

Опираясь на опыт разработки ведущих компаний по созданию АС, основанных на терминальной архитектуре, мы предлагаем проект АС на базе сервера «Aquarius N73 Q42»:

- регистрационный номер сертификата соответствия: СФ/СЗИ-0204;
- срок действия сертификата соответствия: 20.03.2018 – 20.03.2023;
- условное наименование (индекс): «Сервер «Aquarius N73 Q42» (№ 2150916096301 - 0001 (C8280FE05MA0035));
- выполняемая функция соответствует требованиям ФСБ России по безопасности информации, предъявляемым к защищённым средствам вычислительной техники 2 категории, эксплуатируемым в выделенных помещениях, и Дополнению № 2 к ним (по 3 классу защищённости). А также может использоваться в выделенных помещениях до 2 категории включительно на территории Российской Федерации, в том числе органов государственной власти Российской Федерации, для обработки информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований руководства по эксплуатации РЭ 4012 – 026 - 55017660-2016;
- изготовитель: ООО «Производственная компания Аквариус» 105082, Москва, Спартаковская площадь, д. 14, стр. 1.

Проведя анализ рынка предложений тонких клиентов с учетом специфики предприятий оборонной промышленности, предлагаем в нашем проекте АС использовать тонкий клиент ЭТОНК 1900.

Назначение ЭТОНК 1900 – обеспечение доверенной загрузки тонкого клиента и контроля целостности, идентификации и аутентификации пользователя до передачи управления операционной системе.

Преимущества ЭТОНК 1900:

- программная реализация, не требующая аппаратных средств;
- единственное на рынке средство доверенной загрузки, позволяющее противостоять атакам, направленным на модификацию BIOS;
- экономичность и доступная цена, связанная с отсутствием дополнительных аппаратных компонентов;
- возможность применения в любых бизнес-процессах, основанных на технологиях «клиент – сервер»;
- востребованность в медицинских, образовательных, муниципальных и учреждениях здравоохранения.

Технические характеристики ЭТОНК 1900 приведены в таблице.

Технические характеристики ЭТОНК 1900

Операционная система	Astra Linux Special Edition Релиз Смоленск
Процессор	Intel Celeron Processor J1900 (2M кэш, до 2.42GHz), 4 ядра
Память	RAM DDR3L 4Gb
Графический адаптер	Intel HD Graphics, максимальное разрешение: 1920x1080@60GHz
Интерфейсы	• DVI-I (2 Монитора) • DP • Разъем для наушников/микрофона • 5x USB2.0 • 1x USB3.0 • Gigabit Ethernet (RJ-45) 10/100/1000

Сертификаты ЭТОНК 1900:

– сертификат Минобороны России № 815, подтверждающий выполнение требований Приказа МО РФ, в том числе:

- руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 3 классу защищенности от несанкционированного доступа к информации (в части требований «идентификации и аутентификации») подсистемы управления доступом и «целостность КСЗ» подсистемы обеспечения целостности;
- руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (Гостехкомиссия России, 1999) – по 2 уровню контроля;
- криптографических и инженерно-криптографических требований к программным датчикам случайных чисел, используемых в средствах защиты информации объектов вычислительной техники Вооруженных Сил Российской Федерации;
- по соответствию реальных и декларируемых в документации функциональных возможностей;
- задания по безопасности ИЦ-ЭШ.586.

– ФСТЭК России № 1872, подтверждающий выполнение требований руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (Гостехкомиссия России, 1999) – по 2 уровню контроля.

В качестве операционной системы, устанавливаемой на сервере для использования на тонком клиенте ЭТОНК 1900, подключенного к серверу в нашем проекте АС, предлагаем использовать ОС СН. Назначение и преимущества ОС СН описаны выше.

В дополнение к нашему типовому проекту можно использовать:

- программно-аппаратный комплекс доверительной загрузки «Соболь»;
- регистрационный номер сертификата соответствия: СФ/527-2623;
- срок действия сертификата соответствия: 30.06.2015 – 01.06.2020;
- условное наименование (индекс): «Программно-аппаратный комплекс «Соболь». Версия 3.0»;
- соответствует требованиям ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ класса 1Б и может использоваться для защиты от несанкционированного доступа к информации, содержащей/не содержащей сведений, составляющих государственную тайну;
- изготовитель: ООО «Код Безопасности» 129075, Москва, Мурманский проезд, д. 14, корп. 1.

– аппаратно-программный модуль доверенной загрузки «Тринити»:

- регистрационный номер сертификата соответствия: СФ/027-2527;
- срок действия сертификата соответствия: 25.12.2014 – 31.08.2019;
- условное наименование (индекс): «Аппаратно-программный модуль доверенной загрузки «Тринити АПМДЗ-С»;
- соответствует требованиям ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ класса 2Б и может использоваться для защиты от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну;
- изготовитель: ООО Фирма «Инфо Крипт» 119526, Москва, пр-т Вернадского, д. 105, к. 2.

Литература

1. Петухов Р. Н. Применение технологии «тонкий клиент» на промышленных предприятиях // «Молодой учёный». № 17 (121). Сентябрь 2016 г. С. 71–74.

2. Утвержден РУСБ.10015-01-УД. Операционная система специального назначения «Astra linux special edition» // Руководство по КЗС. Часть 1. РУСБ.10015-01 97 01-1. Январь 2015 г. С. 1-138.