В ЭТОМ КАТАЛОГЕ ПРЕДСТАВЛЕНЫ СЛЕДУЮЩИЕ ПРОДУКТОВЫЕ ЛИНЕЙКИ РАЗРАБОТКИ ОКБ САПР

◇ Средства доверенной загрузки

- **ПАК «Аккорд-АМДЗ»** – аппаратный модуль доверенной загрузки;
- **ПАК «Инаф»** – аппаратный модуль доверенной загрузки с USB-интерфейсом.
- **Аккорд-МКТ** – модуль доверенной загрузки для компьютеров на базе процессоров RockChip, Байкал, Эльбрус и других, отличных от x86.

◇ Средства разграничения доступа

- **ПАК «Аккорд-Win32» (TSE) и ПАК «Аккорд-Win64» (TSE)** – программно-аппаратный комплекс разграничения доступа пользователей к информационным ресурсам в среде ОС семейства Windows, включая функцию доверенной загрузки ОС;
- **СПО «Аккорд-Win64 К» –** специальное программное обеспечение разграничения доступа пользователей к информационным ресурсам в среде ОС семейства Windows без реализации функции доверенной загрузки;
- **ПАК «Аккорд-Х» –** программно-аппаратный комплекс разграничения доступа пользователей к информационным ресурсам в среде 32-х разрядных ОС семейства Linux;
- **СПО «Аккорд-Х К» –** специальное программное обеспечение разграничения доступа пользователей к информационным ресурсам в среде ОС семейства Linux, без реализации функции доверенной загрузки;
- **ПАК «Аккорд-XL»** – программно-аппаратный комплекс разграничения доступа пользователей к информационным ресурсам в среде как 32-х, так и 64-х разрядных ОС семейства Linux.

◇ Средства защиты инфраструктур виртуализации

- **«Аккорд-В.» –** средство защиты инфраструктуры виртуализации VMware vSphere 5, 5.1, 5.5, 6.0, 6.5;
- **«Сегмент-В.» –** инструмент управления доступом к системе управления виртуальной инфраструктурой VMware;
- **«ГиперАккорд»** – средство защиты инфраструктур виртуализации, построенных на базе Hyper-V версии 2 и 3.
- **«Аккорд-KVM»** – средство защиты инфраструктур виртуализации, построенных на базе KVM.

◇ Средства защиты информации при удаленной работе пользователей

- **ПАК «Центр-Т»** – программно-аппаратный комплекс для обеспечения защищенной загрузки образов программного обеспечения терминальных станций по сети;
- **СОДС «МАРШ!» –** программно-аппаратный комплекс для организации защищённой работы удалённых пользователей недоверенных компьютеров с сервисами доверенной распределенной информационной системы через сети передачи данных в рамках доверенного сеанса связи.

◇ Средства вычислительной техники в защищенном исполнении и АРМ на их основе

Микрокомпьютеры Новой гарвардской архитектуры

- **«МКТ-card» и «МКТ-card long»** – доверенные микрокомпьютеры Новой гарвардской архитектуры в виде стационарной док-станции и отчуждаемого компьютера;
- **«m-TrusT»** – одноплатный компьютер Новой гарвардской архитектуры для обеспечения защищенной сетевой коммуникации между элементами критической информационной инфраструктуры.
- **«TrusTPad»** – планшет Новой гарвардской архитектуры, позволяющий с помощью физического переключателя выбрать режим работы – защищенный или незащищенный.

Автоматизированные рабочие места (АРМ), построенные на платформе описанных СВТ и СЗИ

- **ПАК «Ноутбук руководителя»** – программно-аппаратный комплекс для защищенной работы пользователей ноутбуков с сервисами доверенной распределенной информационной системы через сеть Интернет в рамках доверенного сеанса связи;
- **Двухконтурный моноблок** – защищенное АРМ на базе микрокомпьютера МКТ-card long для защищенной работы параллельно в двух изолированных один от другого контурах информационной системы;
- **КМ** – криптомаршрутизатор объектового уровня на базе микрокомпьютера МКТ-card long или в исполнении в стойку (в виде одноюнитового сервера) на базе Новой гарвардской архитектуры;
- **СХСЗ на базе МКТ-card long** – сервер хранения и сетевой загрузки для применения в инфраструктуре Центр-Т, не требующий установки в стойку;
- **Защищенный терминал** – парадигма АРМ типа «защищенный терминал» на базе микрокомпьютера МКТ-card long.

◇ Средства управления защитой информации

- **СУЦУ** – система удаленного мониторинга и централизованного управления комплексами «Аккорд».

◇ Средства защиты данных на съемных носителях

- **ПАК «Секрет фирмы»** – программно-аппаратный комплекс, который обеспечивает централизованное управлением применением защищенных СНИ в режиме реального времени в рамках корпоративной сети, а применение их вне корпоративной сети – исключает;
- **ПАК «Секрет особого назначения»** – защищенный СНИ с системой аппаратного журналирования всех попыток подключения носителей.
- **USB-накопитель «Транзит»** – USB-накопитель без возможности перепрограммирования его внутреннего ПО.

- **ПАК «ПАЖ»** – защищенный СНИ**,** предназначенный для ведения неперезаписываемого журнала событий различных приложений.
- **ПАК «Идеальный токен»** – токен с функцией ограничения числа компьютеров, на которых возможно его применение.
- **Мобильный носитель лицензий** – USB-устройство, позволяющее генерировать лицензии на ПО без передачи сведений об информационной системе эксплуатирующей организации производителю ПО.

◇ Средства интеграции с системой видеомониторинга

- **Универсальный хаб «Рассвет»** – периферийное устройство, подключаемое к USB-хосту контроллера «Аккорд» или USB-хосту СВТ для интеграции со смежными и управляющими системами;
- **Комплекс интеграции СЗИ НСД с системой видеомониторинга и контроля доступа «Рассвет-СВМиКД»** – комплекс, предназначенный для управления доступом пользователей к ресурсам подконтрольных объектов;
- **Сервер интеграции СЗИ НСД и систем видеомониторинга и контроля доступа** – управляющий компонент, обеспечивающий взаимодействие серверов СЗИ НСД и серверов СКУД при интеграции на уровне объединения объектов доступа и логического взаимоувязывания помещений и компьютеров.

◇ Идентификаторы пользователя и считыватели идентифицирующей и/или аутентифицирующей информации

- **ПИ ШИПКА** – персональный идентификатор пользователя;
- **Биометрические считыватели** – считыватели биометрических данных пользователя (сосудистого русла ладони).

СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ

ПАК «АККОРД-АМДЗ»

Общие сведения

ПАК «Аккорд-АМДЗ» – это аппаратный модуль доверенной загрузки (далее – «Аккорд-АМДЗ»), представляющий собой в терминах российской нормативной методической базы средство доверенной загрузки уровня платы расширения.

Все модификации комплекса поддерживают файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, QNX4, MINIX. Доверенная загрузка выполняется для ОС типа MS DOS, Windows, QNX, OS/2, UNIX, LINUX, BSD, vSphere и др.

Поддерживается работа с аппаратными идентификаторами пользователя.

Персональные идентификаторы и съемники информации для всех наших продуктов заказываются отдельно из списка поддерживаемых на данный момент (список постоянно расширяется, в том числе и по запросам эксплуатирующих организаций).

Основные возможности

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки ОС, и обеспечивает доверенную загрузку ОС, использующих одну из поддерживаемых файловых систем.

«Доверенная загрузка» – это загрузка заранее определенной ОС в неизмененном виде из известного источника известным пользователей. То есть загрузка только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации /аутентификации пользователя.

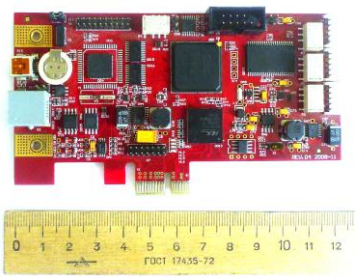
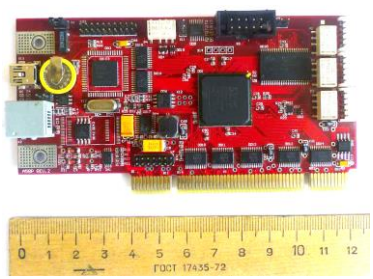
Особенности

«Аккорд-АМДЗ» может быть реализован на различных контроллерах, но его базовая функциональность всегда остается одинаковой и соответствует заявленной и отраженной в сертификатах соответствия.

Для того чтобы выбрать нужный вариант, необходимо определить свободный слот с типом шинного интерфейса у СВТ, в которое планируется установить «Аккорд-АМДЗ».

Это может быть:

- PCI или PCI-X – контроллеры Аккорд-5.5;
- PCI-express – контроллеры Аккорд-5.5.e, Аккорд-GX;
- Mini PCI-express – контроллеры Аккорд-GXM, Аккорд-GXMH;
- m.2 – контроллер Аккорд-GXM2.

	
Аккорд-5.5e	*Аккорд-5.5*
	
Аккорд-GX	*Аккорд-GXM*

	
Аккорд-GXMH	*Аккорд-GXM2*

Контроллеры «Аккорд-АМДЗ»

Все контроллеры допускают возможность расширения функций от «Аккорда-АМДЗ» до ПАК «Аккорд-Win32» / «Аккорд-Win64» / «Аккорд-X (XL)»). Можно выбирать «Аккорд-АМДЗ» на базе любого контроллера, не опасаясь, что если в дальнейшем Вам понадобится добавить ПО разграничения доступа, компоненты окажутся несовместимы.

«Аккорд-АМДЗ» с сертификатом ФСБ выполнен по особым Техническим условиям, в которых предъявлен ряд дополнительных требований, поэтому, если требуется именно такой Аккорд, при оформлении заказа необходимо выбрать строку с примечанием «сертификат ФСБ». Он отличается, в частности тем, что в нем возможность отключения питания компьютера в случае, если за **N** секунд не начал работу **BIOS** модуля доверенной загрузки (так называемый «сторожевой таймер») реализована как обязательная, а не опциональная функция.

PCI- и USB-устройства ОКБ САПР являются легальными, VendorID ОКБ САПР для устройств обоих типов: 1795.

ПАК «ИНАФ»[1]

Общие сведения

СДЗ «Инаф»

ПАК «Инаф» (далее – «Инаф») – это аппаратный модуль доверенной загрузки на шине USB, представляющий собой в терминах нормативной методической базы средство доверенной загрузки платы расширения.

Комплекс «Инаф» поддерживает файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX. Доверенная загрузка выполняется для ОС типа MS-DOS, ОС семейства Windows, QNX, OS/2, UNIX, LINUX, BSD и др.

Поддерживается работа с аппаратными идентификаторами пользователя.

Персональные идентификаторы и съемники информации заказываются отдельно.

Основные возможности

«Инаф» обеспечивает выполнение всех основных функций аппаратного модуля доверенной загрузки:

- аппаратный контроль целостности технических, программных средств, условно-постоянной информации СВТ до загрузки ОС, с реализацией пошагового алгоритма контроля;
- возможность доверенной загрузки ОС, а также системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска СВТ нескольких ОС;
- автоматическое ведение протокола регистрируемых событий на этапе доверенной загрузки ОС (в системном

[1] Enough (англ.) – достаточно. Произносится [ináf].

журнале, размещенном в энергонезависимой памяти аппаратной части комплекса);

- администрирование встроенного ПО комплекса (генерацию пароля администратора и определение его параметров; назначение файлов для контроля целостности и режимов контроля, работу с журналом регистрации системных событий, контроль аппаратной части СВТ) и разделение прав администратора безопасности информации комплекса и пользователя СВТ;
- регистрация, сбор, хранение и выдача данных о событиях, происходящих в СВТ в части системы защиты от несанкционированного доступа.

Особенности

Программно-информационная часть комплекса, включающая firmware контроллера, базу контроля целостности, базу пользователей, журнал регистрации событий и средства администрирования, размещена в энергонезависимой памяти контроллера. Этим обеспечивается возможность проведения процедур контроля целостности технических и программных средств СВТ, администрирования и аудита средствами «Инаф» на аппаратном уровне до загрузки ОС.

В зависимости от конструктивных возможностей СВТ возможна как установка контроллера «Инаф» внутри корпуса СВТ в качестве штатного устройства с USB-разъемом типа A, так и подключение к штырьково-му разъему непосредственно на материнской плате СВТ. «Инаф» с таким типом подключения может быть выполнен с «коленом» под прямым углом.

«Инаф» штырьковый

Поскольку контроллер «Инаф» реализован в форм-факторе USB-устройства, он не требует для своей установки наличия на СВТ свободного PCI-слота и может применяться

в случаях, когда используются blade-серверы, в которых отсутствуют PCI-слоты, но имеются свободные внутренние или внешние USB-разъемы.

Перед началом работы с «Инаф» необходимо настроить в BIOS компьютера загрузку с контроллера «Инаф» как с жесткого диска.

Во время старта компьютера «Инаф» получает управление, проводит процедуры контроля целостности аппаратуры и файлов, и в случае успешного завершения данной процедуры передает управление ОС на диске.

«Инаф» может использоваться в рамках реализации двух типов сценариев:

Стационарная установка в СВТ

Данный тип сценария используется в том случае, когда необходима непрерывная реализация функционала «Инаф». В этом случае контроллер соответствующим образом настроен и подключен к USB-порту СВТ постоянно. Каждый раз перед загрузкой ОС пользователем СВТ контроллер «Инаф» выполняет процедуру контроля целостности определенных заранее объектов. В случае нарушения целостности загрузка ОС блокируется и требуется вмешательство администратора безопасности информации (пользователя «Инаф»).

Для корректного осуществления работы по данному типу сценария необходимо:

- установить в BIOS вариант загрузки с «Инаф» как с жесткого диска;
- установить пароль на вход в BIOS;
- принять административные меры, исключающие несанкционированное отключение устройства от USB-порта:
- ограничить физический доступ к СВТ и/или зафиксировать устройства с помощью специальных креплений и/или голографической наклейки или установить контроллер внутрь корпуса СВТ.

Использование в качестве мобильного устройства

Данный тип сценария используется в том случае, когда нет необходимости выполнять процедуры контроля целостности объектов постоянно и запрещать для пользователей СВТ загрузку ОС в случае нарушения целостности, а нужно только выявить сам факт нарушения целостности установленных на контроль объектов.

В этом случае сначала выполняются все необходимые настройки подключенного к СВТ контроллера «Инаф», затем контроллер извлекается из СВТ и хранится в надежном месте (например, в сейфе). Пользователи СВТ работают в обычном режиме, а пользователь «Инаф» периодически подключает к СВТ свой контроллер «Инаф» с целью убедиться в неизменности состава СВТ и установленных ранее на контроль объектов.

Возможен также вариант работы с «Инаф», когда контроллер подключается к СВТ каждый раз перед началом сеанса работы и извлекается из СВТ после ее выключения.

Для корректного осуществления работы по данному типу сценария обязательно должны быть предусмотрены специальные регламенты действий пользователей, в чьи обязанности входит запуск СВТ, так как наличие «Инаф» в USB-порту должны контролировать именно они.

Следует помнить о том, что поскольку для работы с «Инаф» требуется настраивать порядок загрузки ОС в BIOS компьютера, необходимо накладывать определенные ограничения (особенно в случае стационарной установки «Инаф» в СВТ) на доступ пользователей СВТ к BIOS (путем установки пароля на BIOS).

СДЗ УРОВНЯ BIOS «АККОРД-МКТ»

Модуль доверенной загрузки «Аккорд-МКТ» является средством доверенной загрузки (СДЗ) для компьютеров, построенных на процессорах RockChip, Байкал, Эльбрус и других, отличных от x86.

МДЗ «Аккорд-МКТ» является программным продуктом (специальным программным обеспечением, СПО), предназначенным для встраивания в базовую систему ввода-вывода (БСВВ) микрокомпьютеров (далее по тесту – микрокомпьютер либо МКТ) и обеспечения выполнения основных функций его защиты от НСД, в том числе настройки, контроля функционирования и управления защитными механизмами.

Встраивание (прошивка) СПО «Аккорд-МКТ» в БСВВ выполняется производителем изделия на этапе изготовления МКТ, то есть «Аккорд-МКТ» приобретается в составе микрокомпьютера.

Возможности

МДЗ «Аккорд-МКТ» обеспечивает:

1. идентификацию и аутентификацию пользователей при входе в систему по уникальному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
2. идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования МДЗ «Аккорд-МКТ» по уникальному идентификатору пользователя и по паролю 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
3. контроль целостности отдельных файлов и программных средств МКТ;
4. администрирование, включающее:
   - регистрацию пользователей и их идентификаторов;
   - построение списков объектов для контроля целостности и указание режимов контроля;

- работу с журналом регистрации системных событий и действий пользователей.

5. возможность резервного копирования на отчуждаемый носитель и восстановления базы данных пользователей и списка контролируемых объектов;

6. регистрацию и учет системных событий и действий пользователей.

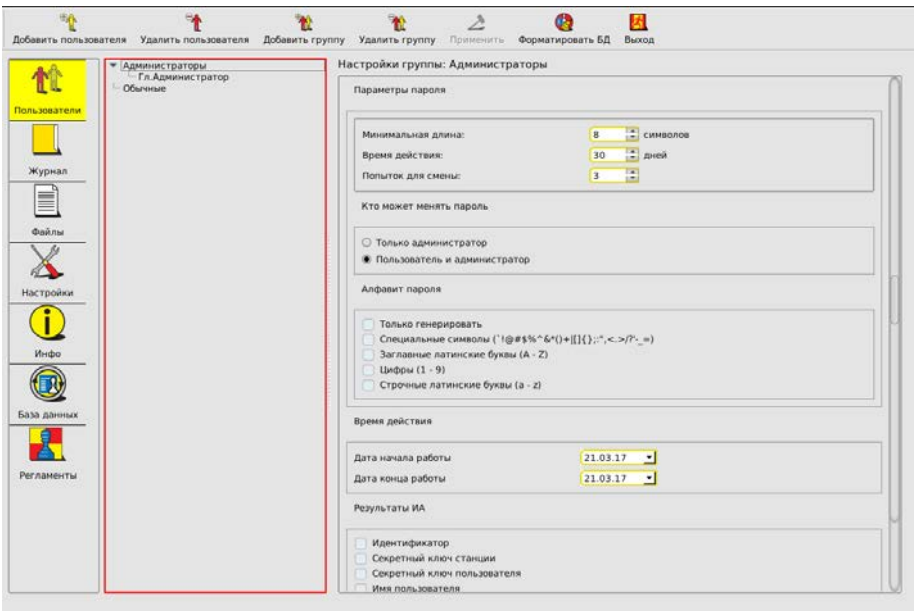


Рисунок 4 – Главное окно интерфейса администрирования

Пользователь МДЗ «Аккорд-МКТ», как и пользователи других СДЗ, не столько применяет это средство защиты, сколько работает под его контролем. Взаимодействие пользователя с «Аккорд-МКТ» сводится к идентификации, аутентификации и смене пароля (по истечении срока действия или в произвольный момент времени). Остальные контрольные процедуры проводятся МДЗ самостоятельно.

Администратор МДЗ «Аккорд-МКТ», как и администраторы других СДЗ, осуществляет регистрацию пользователей и настройку защитных средств МДЗ «Аккорд-МКТ».

Графический интерфейс и логика работы с «Аккорд-МКТ» не имеет существенных отличий от «Аккорда-АМДЗ», поэтому тем, кто имеет опыт работы с другими Аккордами, переход на «Аккорд-МКТ» не составит сложностей.

Основные характеристики

Контрольные процедуры делятся на обязательные, которые по умолчанию выполняются при каждом запуске микрокомпьютера, и опциональные, которые устанавливаются администратором БИ.

К обязательным процедурам контроля относятся:

1. процедура идентификации оператора (пользователя);
2. процедура аутентификации (подтверждение достоверности) оператора (пользователя);
3. проверка целостности отдельных файлов и программных средств МКТ.

К опциональным процедурам контроля относятся:

4. процедура смены пароля, выполняемая, когда время жизни пароля превысило установленный администратором БИ интервал времени;
5. проверка ограничения на время входа оператора (пользователя) в систему.

Особенности и условия применения

СПО «Аккорд-МКТ» встраивается производителем в БСВВ микрокомпьютера на этапе изготовления и функционирует в его составе. Среда функционирования МДЗ «Аккорд-МКТ» должна запрещать любые действия от имени пользователя до завершения процедур идентификации и аутентификации пользователя, требовать выполнения данных процедур до разрешения любого действия, а также должна быть способна предоставлять надежные метки времени.

СРЕДСТВА РАЗГРАНИЧЕНИЯ ДОСТУПА

ПАК «АККОРД-WIN32» (TSE) И ПАК «АККОРД-WIN64» (TSE)

Общие сведения

ПАК «Аккорд-Win32» (TSE) и ПАК «Аккорд-Win64» (TSE) предназначены для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам. Комплекс работает на всей ветви ОС Microsoft NT+, на терминальных серверах, построенных на базе ОС Windows (32-х разрядных для ПАК «Аккорд-Win32» и 64-х разрядных для ПАК «Аккорд-Win64»), и терминального ПО Citrix, работающего на этих ОС, работающем на этих ОС. Поддерживаются аппаратные идентификаторы пользователей.

Возможности

1. Защита от несанкционированного доступа к СВТ;
2. идентификация/аутентификация пользователей до загрузки ОС с последующей передачей результатов успешной идентификации/аутентификации в ОС;
3. аппаратный контроль целостности системных файлов и критичных разделов реестра;
4. доверенная загрузка ОС;
5. контроль целостности программ и данных, их защита от несанкционированных модификаций;
6. создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
7. запрет запуска неразрешенных программ;
8. разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
9. разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;

10. автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса;

11. идентификация/аутентификация пользователей, подключающихся к терминальному серверу;

12. опциональная автоматическая идентификация в системе Windows NT+ и на терминальном сервере пользователей, аутентифицированных защитными механизмами контроллера «Аккорд-АМДЗ» (при таком подходе, избегая повторной идентификации пользователей, можно гарантировать, что ОС будет загружена под именем того же пользователя, который был аутентифицирован в контроллере «Аккорд-АМДЗ», и к терминальному серверу подключится тот же самый пользователь);

13. управление терминальными сессиями (настройка реакции на отключение идентификатора от терминала (блокировка / отключение / сохранение сессии));

14. контроль печати на принтерах, подключенных как к терминальным серверам, так и к пользовательским терминалам, который позволяет протоколировать вывод документов на печать и маркировать эти документы (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация);

15. контроль доступа к USB-устройствам.

Особенности

1. Собственная система разграничения доступа (мандатный и дискреционный методы контроля) – действия, разрешенные настройками разграничения доступа операционной системы, но запрещенные комплексом, будут запрещены пользователю;

2. Комплекс включает в себя компоненты, устанавливаемые как на сервер, так и на клиентское СВТ: «Аккорд-ТС» (Терминальный сервер) и «Аккорд-ТК» (терминальный клиент)). Эти компоненты взаимодействуют между собой при старте сессии, создавая виртуальный канал и передавая по нему аутентифицирующие данные. Это

обеспечивает уверенность в том, что с защищенным терминальным сервером взаимодействуют только те терминалы, на которые также установлены компоненты комплекса, а не любые произвольные СВТ;

3. возможность использовать уже установленную связь (на протоколах RDP и ICA) между сервером и терминалом, а не устанавливать новую;

4. в течение всего сеанса работы пользователя ведется подробный журнал событий, в котором фиксируются все действия пользователя на терминальном сервере;

5. ПО комплекса позволяет администратору безопасности информации описать любую не противоречивую политику безопасности на основе наиболее полного набора атрибутов:

Операции с файлами	
R	разрешение на открытие файлов только для чтения
W	разрешение на открытие файлов для записи
C	разрешение на создание файлов на диске
D	разрешение на удаление файлов
N	разрешение на переименование файлов
V	видимость файлов
O	эмуляция разрешения на запись информации в открытый файл
Операции с каталогами	
M	создание каталогов на диске
E	удаление каталогов на диске
G	разрешение перехода в этот каталог

n	переименование подкаталогов
S	наследование прав на все вложенные подкаталоги
1	наследование прав на 1 уровень вложенности
0	запрет наследования прав на все вложенные подкаталоги
Прочее	
X	разрешение на запуск программ
Регистрация	
r	регистрация в журнале операций чтения при обращении к объекту
w	регистрация в журнале операций записи при обращении к объекту

меток доступа, которые могут быть поименованы как уровни секретности либо другим, более удобным образом (количество меток допуска может достигать шестнадцати), и параметров:

- перечень файлов, целостность которых должна контролироваться системой, и опции контроля;
- запуск стартовой задачи (для функционально замкнутых систем);
- наличие либо отсутствие привилегий супервизора (при этом каждому администратору безопасности назначается любой необходимый перечень привилегий, например, можно настроить систему таким образом, чтобы у 3 разных администраторов безопасности были права выполнения непересекающихся перечней настроек, то есть настройки, доступные одному, будут недоступны двум остальным);
- детальность журнала доступа;
- назначение/изменение пароля для аутентификации;

- временные ограничения – время по дням недели (с дискретностью 30 мин), в которое разрешено начало работ для данного субъекта;
- параметры управления экраном – гашение экрана через заранее определенный интервал времени (в случае, если в течение указанного интервала действия оператором не выполнялись), подача соответствующих звуковых и визуальных сигналов.

Возможно использование вместо пароля (или одновременно с паролем) биометрической аутентификации пользователя.

Сильной стороной продукта является возможность контроля печати, как на сетевых принтерах, так и на локальных, с протоколированием вывода документов на печать и их маркировки. Данные настройки работают при печати документов из любого прикладного программного обеспечения, предусматривающего возможность вывода документа на печать (не только Microsoft Office). В качестве маркера может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация (рисунок 5).

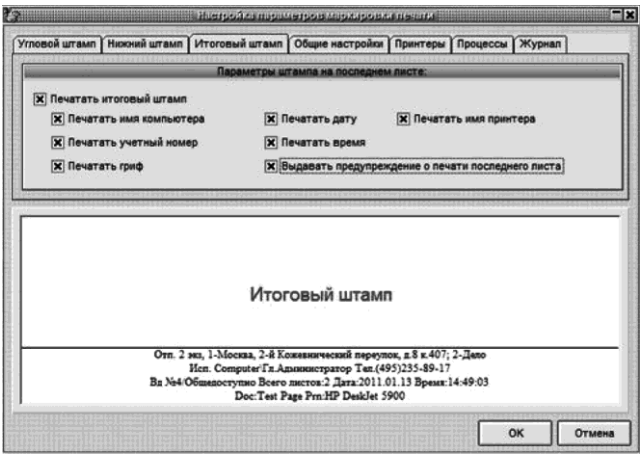


Рисунок 5 – Параметры маркировки печати

СПО «АККОРД-WIN64 K»

Общие сведения

На сегодняшний день многие организации используют программно-аппаратные комплексы средств защиты информации ПАК «Аккорд-Win32» и ПАК «Аккорд-Win64», разработанные ОКБ САПР. С их помощью можно реализовать следующие основные функции безопасности:

- доверенная загрузка компьютера;
- идентификация/аутентификация пользователя;
- контроль целостности системной области диска, системных файлов, программ и данных;
- разграничение доступа пользователей к ресурсам компьютера;
- ведение протокола регистрируемых событий.

Однако для некоторых систем доверенная загрузка компьютера не является необходимой для реализации. К таким относятся:

- системы, для которых необходима защита информационных ресурсов от несанкционированного доступа, а целостность критичных файлов ОС уже достоверно подтверждена до загрузки ОС (например, с помощью «Инаф») или обеспечена технологически;
- системы, в которых для удовлетворения требований по безопасности не требуется обеспечение доверенной загрузки средств вычислительной техники. Это государственные информационные системы (ИС), в которых обрабатывается информация минимального уровня значимости, или государственные ИС регионального или объектового масштаба, в которых обрабатывается информация низкого уровня значимости (в соответствии с приказом ФСТЭК № 17), а также ИС персональных данных 3 и 4 уровня защищенности (в соответствии с приказом ФСТЭК № 21).

В таких случаях при применении ПАК «Аккорд-Win32»/ «Аккорд-Win64» набор функций защиты будет избыточным. Поэтому компанией ОКБ САПР был разработан комплекс, реализующий все функции ПАК «Аккорд-Win32»/

«Аккорд-Win64», кроме функции доверенной загрузки, не требуемой для указанных систем — СПО «Аккорд-Win64 K».

СПО «Аккорд-Win64 K» предназначено для разграничения доступа к рабочим станциям, терминалам, терминальным серверам в 32-х и 64-х разрядных ОС семейства Windows. Разрядность ОС указывается при начале инсталляции СПО.

Комплекс работает на рабочих станциях под управлением ОС Windows NT / XP / Vista / 7 / 8, и на терминальных серверах на базе ОС Windows 2000 / 2003 / 2008 / 2012 R2.

Предусмотрена идентификация / аутентификация пользователя с помощью ТМ-идентификаторов DS 199x, ПИ ШИПКА или смарт-карт.

Возможности

1. Защита от несанкционированного доступа;
2. идентификация/аутентификация пользователей для входа в ОС;
3. статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
4. запрет запуска неразрешенных программ;
5. разграничение доступа пользователей с помощью дискреционного контроля доступа;
6. разграничение доступа пользователей и процессов с помощью механизма контроля доступа на основе иерархических меток;
7. регистрация событий;
8. управление терминальными сессиями;
9. контроль печати на сетевых и локальных принтерах;
10. контроль доступа к USB-устройствам.

Особенности

- позволяет установить временной интервал, в который загрузка СВТ запрещена;
- позволяет контролировать целостность системной области диска, системных файлов, программ и данных;
- имеет собственную систему разграничения доступа;
- поддерживает управление потоками информации;

- поддерживает механизм блокировки экрана после некоторого установленного времени неактивности, который дополнен функцией идентификации пользователя при разблокировании СВТ;
- позволяет контролировать печать из любого прикладного ПО и маркировать выводимые на печать документы (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

ПО комплекса позволяет администратору безопасности информации реализовать правила разграничения доступа на основе того же набора атрибутов, меток доступа и параметров, что и комплексы без К.

Также возможно использование вместо пароля (или одновременно с паролем) биометрической аутентификации пользователя.

Сравнение с ПАК «Аккорд-Win32»/ «Аккорд-Win64»

Для реализации функций защиты (в первую очередь доверенной загрузки) ПАК «Аккорд-Win32»/«Аккорд-Win64» использует контроллер. Отсутствие контроллера в составе СПО «Аккорд-Win64 К» обуславливает некоторые различия в реализации функций. Различия рассмотрены в таблице ниже.

Различие	**ПАК «Аккорд-Win32»/ «Аккорд-Win64»**	**СПО «Аккорд-Win64 К»**
Способ реализации процедур контроля целостности	Аппаратный, программный	Программный
Время проведения процедур контроля целостности в поэтапной загрузке компьютера	Выполняется до и после загрузки ОС	Выполняется после загрузки ОС

Время проведения процедур идентификации /аутентификации	Выполняется до загрузки ОС	Выполняется при загрузке ОС
Хранение эталонных значений контрольных сумм	В энергонезависимой памяти контроллера	На жестком диске компьютера
Хранение идентификационной информации пользователей	В энергонезависимой памяти контроллера	На жестком диске компьютера

ПАК «АККОРД-Х»

Общие сведения

ПАК «Аккорд-Х» предназначен для разграничения доступа пользователей к рабочим станциям под управлением ОС семейства Linux.

В качестве идентификатора пользователя могут использоваться ТМ, ПИ ШИПКА.

Возможности

1. Защита от несанкционированного доступа к ПК (включая возможность ограничения разрешенных часов работы каждого пользователя);
2. идентификация/аутентификация пользователей до загрузки операционной системы с возможностью последующей передачи результатов успешной идентификации/аутентификации в ОС;
3. аппаратный контроль целостности системных файлов;
4. доверенная загрузка ОС;
5. статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
6. разграничение доступа пользователей, процессов, к массивам данных (объектам) с помощью дискреционного контроля доступа;

7. разграничение доступа пользователей, процессов, к массивам данных (объектам) с помощью мандатного контроля доступа;

8. разграничение доступа пользователей, к определенным процессам;

9. контроль доступа к периферийным устройствам;

10. создание индивидуальной для каждого пользователя изолированной рабочей программной среды;

11. автоматическое ведение протокола регистрируемых событий;

12. контроль печати на локальных и сетевых принтерах, протоколирование вывода данных на печать, маркировка распечатанных данных (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

Особенности

1. Наличие собственной системы разграничения доступа (мандатный и дискреционный методы контроля доступа) – действия, разрешенные прикладным ПО, но запрещенные комплексом будут запрещены пользователю;

2. в течение всего сеанса работы пользователя ведется подробный журнал событий, в котором фиксируются все действия пользователя (существует возможность настраивать уровень детальности журнала);

3. ПО комплекса позволяет администратору безопасности информации описать любую не противоречивую политику безопасности на основе наиболее полного набора атрибутов:

Дискреционные ПРД для объектов	
R	разрешение на открытие объекта только для чтения
W	разрешение на открытие объекта для записи
X	разрешение на открытие объекта на выполнение

O	подмена атрибута R атрибутами RW на этапе открытия объекта (эмуляция разрешения на запись информации в открытый файл)
C	разрешение на создание объекта
D	разрешение на удаление объекта
N	разрешение на переименование объекта
L	разрешение на создание жесткой ссылки для объекта
I	разрешение на создание симлинка для объекта или контейнера
Дискреционные ПРД для контейнеров	
M	создание каталогов на диске
E	удаление каталогов на диске
G	разрешение перехода в этот каталог
n	переименование подкаталогов
S	наследование прав на все вложенные подкаталоги
1	наследование прав на 1 уровень вложенности
0	запрет наследования прав на все вложенные подкаталоги

меток доступа, которые могут быть поименованы как уровни секретности либо другим, более удобным образом (количество меток допуска может достигать шестнадцати) и параметров:

- перечень объектов и прав доступа к ним для конкретного субъекта;
- перечень объектов и прав доступа к ним для группы субъектов;

- перечень объектов, целостность которых должна контролироваться системой (статический и/или динамический контроль целостности) для конкретного субъекта;
- перечень объектов, целостность которых должна контролироваться системой (статический и/или динамический контроль целостности), для группы субъектов;
- перечень системных возможностей субъекта;
- перечень системных настроек;
- уровень детальности журнала регистрации событий;
- назначение/изменение пароля для аутентификации;
- назначение/изменение идентификатора;
- временные ограничения – время по дням недели (с дискретностью 30 мин), в которое разрешено начало работ для данного субъекта.

Сильной стороной комплекса является наличие модуля контроля печати, который предоставляет возможность маркировки данных, выводимых на печать на сетевых и локальных принтерах, с протоколированием всех действий пользователя. Модуль контроля печати ПАК «Аккорд-X» отрабатывает при печати документов из любого прикладного программного обеспечения, предусматривающего возможность вывода документа/файлов/данных на печать (не только OpenOffice и прочих текстовых редакторов). Контроль печати осуществляется на уровне подсистемы печати Linux, поэтому данные выводимые на печать из консоли также маркируются в соответствии с настройками подсистемы контроля печати ПАК «Аккорд-X».

В качестве маркера (штампа) может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация.

СПО «АККОРД-Х К»

Общие сведения

СПО «Аккорд-Х К» предназначен для разграничения доступа к рабочим станциям, функционирующим под управлением ОС семейства Linux.

Возможности

1. Защита от несанкционированного доступа;
2. идентификация/аутентификация пользователей для входа в ОС;
3. статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
4. разграничение доступа пользователей к массивам данных и программам с помощью механизма контроля доступа на основе иерархических меток;
5. разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
6. автоматическое ведение протокола регистрируемых событий.

Особенности

СПО «Аккорд-Х К»:

7. позволяет установить предельно допустимый порог неудачных попыток аутентификации;
8. позволяет контролировать целостность системных файлов, программ и данных;
9. имеет собственную систему разграничения доступа;
10. предотвращает доступ к остаточной информации при освобождении (распределении) памяти;
11. поддерживает управление потоками информации, при этом обработка информации определённого уровня конфиденциальности выполняется только с помощью выделенных программ (процессов);

12. позволяет блокировать множество параллельных сессий пользователя;
13. поддерживает механизм блокировки экрана после некоторого установленного времени неактивности, который дополнен функцией идентификации пользователя при разблокировании СВТ;
14. позволяет контролировать печать из любого прикладного программного обеспечения и маркировать выводимые на печать документы (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

Набор атрибутов, меток и параметров доступа комплекса аналогичен набору ПАК «Аккорд-Х».

Сравнение с ПАК «Аккорд-Х»

Для реализации функций защиты (в первую очередь доверенной загрузки) ПАК «Аккорд-Х» использует контроллер. Отсутствие контроллера в составе СПО «Аккорд-Х К» обуславливает некоторые различия в реализации функций. Различия рассмотрены в таблице:

Различие	**ПАК «Аккорд-Х»**	**СПО «Аккорд-Х К»**
Способ реализации процедур контроля целостности	Аппаратный, программный	Программный
Место процедур контроля целостности в поэтапной загрузке компьютера	Выполняется до загрузки ОС и после загрузки ядра ОС	Выполняется после загрузки ядра ОС

Различие	ПАК «Аккорд-Х»	СПО «Аккорд-Х К»
Место процедур идентификации/аутентификации в поэтапной загрузке компьютера	Выполняется до загрузки ОС и в процессе штатной и\а пользователя в ОС	Выполняется в процессе штатной и\а пользователя в ОС
Хранение эталонных значений контрольных сумм	Контрольные суммы файлов, целостность которых проверяется до загрузки ОС, хранятся в ЭНП контроллера, а КС файлов, целостность которых проверяется после загрузки ядра ОС, хранятся в базе данных на жестком диске компьютера	В базе данных на жестком диске компьютера (вариант исполнения 1)/в памяти СОДС «МАРШ!» (вариант исполнения 2)
Хранение идентификационной информации пользователей	Идентификационная информация пользователей «Аккорд-АМДЗ» хранится в энергонезависимой памяти контроллера, идентификационная информация пользователей ПО Аккорд-Х — в базе данных на жестком диске компьютера	В базе данных на жестком диске компьютера (вариант исполнения 1)/в памяти СОДС «МАРШ!» (вариант исполнения 2)

ПАК «АККОРД-XL»

Общие сведения

Подбор и закупка средств защиты информации от несанкционированного доступа, как правило, производится под уже имеющийся в информационной системе парк компьютеров с установленными на них ОС. Одной из характеристик компьютерной системы, знание которой позволяет предъявить к средствам защиты информации вполне определенные требования совместимости, является разрядность ОС. Для систем, использующих единообразно 32-разрядные ОС, подходит программно-аппаратный комплекс ПАК «Аккорд-X».

Однако повсеместно распространена ситуация, когда в организации используются и старые, и новые компьютеры. Старые компьютеры функционируют в основном на 32-разрядных ОС, более новые — на 64-разрядных. В таком случае подходящим вариантом для защиты информации от несанкционированного доступа является другой продукт компании ОКБ САПР — ПАК «Аккорд-XL».

ПАК «Аккорд-XL» предназначен для разграничения доступа к рабочим станциям, функционирующим под управлением 32- и 64-разрядных ОС семейства Linux. Совместимость с различными ОС обеспечивается возможностью выбора при установке дистрибутива для конкретной ОС с той или иной разрядностью. Дальнейшая установка, настройка и использование комплекса ничем не отличается от выполнения тех же процедур при использовании ПАК «Аккорд-X». Комплекс объединяет в своем составе аппаратный компонент — контроллер «Аккорд-АМДЗ», специальное ПО разграничения доступа и средства идентификации пользователя.

Все возможности и особенности ПО, за исключением списка поддерживаемых ОС, совпадают с параметрами ПАК «Аккорд-X».

СРЕДСТВА ЗАЩИТЫ ИНФРАСТРУКТУР ВИРТУАЛИЗАЦИИ

ПАК «АККОРД-В.»

Общие сведения

ПАК «Аккорд-В.» предназначен для защиты виртуальных инфраструктур на базе VMware vSphere версий 5.x и 6.x.

Для приведения защиты виртуальной инфраструктуры в соответствие требованиям регуляторов (руководящие документы и приказы ФСТЭК) важно понимать следующее.

В настоящее время невозможно в полной мере решить все вопросы защиты с использованием всего лишь одного продукта. В свою очередь необходимость использования нескольких решений в большинстве случаев приводит к дублированию функций и проблемам совместимости. Поэтому при проектировании системы защиты требуется продуманная и удобная связка решений.

Слово «связка» использовано не просто так. Можно закрыть требования по защите виртуальных инфраструктур множеством средств, но при этом все равно остаться не защищенными. Например, нельзя доверять антивирусу в ОС, если вирус находится в загрузочном секторе MBR и, как следствие, имеет возможность показывать антивирусу только то, что посчитает нужным.

Чтобы в эффективности средств защиты не приходилось сомневаться, требуется построить доверенную среду, а для этого необходимо придерживаться принципа непрерывности контрольных процедур.

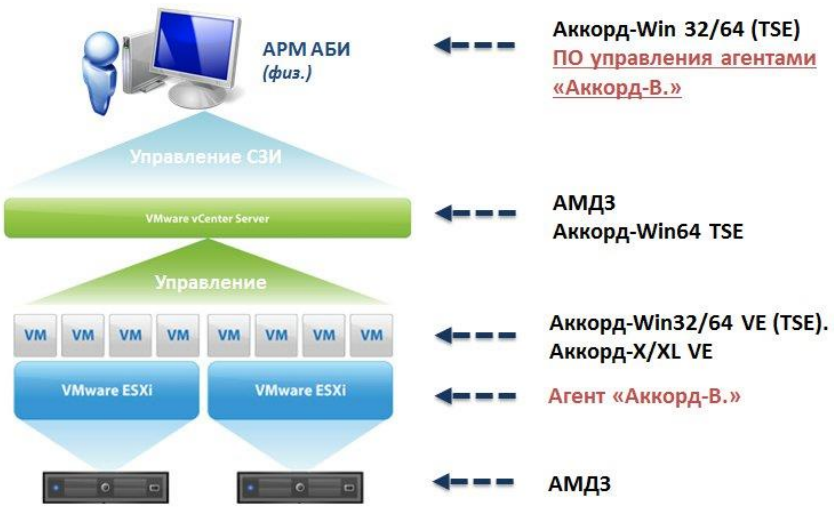
Для обычных, физических АРМ выполнение данного принципа успешно реализуется связкой «Аккорд-АМДЗ + специальное ПО разграничения доступа», но при переходе к виртуальным инфраструктурам этого уже недостаточно. Требуется учитывать «новый слой» и обеспечивать доверенную загрузку виртуальных машин (см. рисунок).

Особенность защиты виртуальных инфраструктур

ПАК «Аккорд-В.» состоит из следующих компонентов:

- «Аккорд-АМДЗ» для физических автоматизированных рабочих мест (в т. ч. серверов). В различных вариациях исполнения от PCI и M2 до USB.
- Системное ПО «Аккорд-В.» – агенты «Аккорд-В.» устанавливаемые на ESXi для осуществления доверенной загрузки виртуальных машин и ПО управления агентами.
- ПАК «Аккорд-Win32»/«Аккорд-Win64»/«Аккорд-X», применяемые для виртуальных машин/физических автоматизированных рабочих мест. Решение применимо как для VDI, так и для терминальных серверов.

Примечание: Терминальная версия содержит в названии TSE. Версия для виртуальных машин содержит в названии VE.



Архитектура системы

Возможности

В ПАК «Аккорд-В.» реализованы следующие механизмы защиты (*приведен список основных возможностей, с полным списком можно ознакомиться в документации на комплекс*):

- Доверенная загрузка и контроль целостности всех элементов инфраструктуры виртуализации;
- Разграничение доступа администраторов виртуальной инфраструктуры и администраторов безопасности информации;
- Разграничение доступа пользователей внутри виртуальных машин;
- Механизмы дискреционного/мандатного контроля доступа пользователей и процессов к защищаемым объектам инфраструктуры виртуализации, включая ресурсы внутри виртуальных машин;
- Механизм очистки оперативной и внешней памяти путём записи маскирующей информации в память при её освобождении (перераспределении);

- Аппаратная идентификация всех пользователей и администраторов инфраструктуры виртуализации.

Важно! Система защиты ПАК «Аккорд-В.» не ограничивает в целях безопасности возможностей виртуальной инфраструктуры, оставляя доступными все ее преимущества.

Особенности

Система защиты ПАК «Аккорд-В.» полностью интегрируется в инфраструктуру виртуализации, поэтому для ее функционирования не требуются дополнительные серверы. При этом ПАК «Аккорд-В.» не ограничивает в целях безопасности возможностей виртуальной инфраструктуры, оставляя доступными все ее преимущества.

ПАК «Аккорд-В.» обеспечивает защищенность всех компонентов среды виртуализации: ESXi-серверов и самих виртуальных машин, серверов управления vCenter, дополнительных серверов со службами VMware (например, VMware Consolidated Backup).

Управление системой защиты осуществляется централизованно с сервера управления виртуальной инфраструктурой. Доступ к инструментам управления системой защиты предоставляется только администраторам безопасности, от администраторов виртуальной инфраструктуры эти инструменты скрыты.

ПАК «Аккорд-В.» закрывает 7 из 10 требований по защите виртуальных инфраструктур приказов ФСТЭК №17 и №21, а именно:

- Идентификация/аутентификация в виртуальной инфраструктуре (ЗСВ. 1)
- Управление доступом (ЗСВ. 2);
- Регистрация событий (ЗСВ. 3);
- Доверенная загрузка (ЗСВ. 5);
- Управление миграцией (ЗСВ. 6);
- Контроль целостности (ЗСВ. 7);
- Сегментирование виртуальной инфраструктуры (ЗСВ.10).

Исключения*:

- Управление потоками (ЗСВ.4);
- Резервирование (ЗСВ.8);
- Антивирусная защита (ЗСВ.9).

**закрываются представленными на рынке решениями*

Законченное решение

ПАК «Аккорд-В.» представляет собой комплексное решение, включающее в себя все необходимые элементы для реализации требований по защите информации.

Отказоустойчивое решение

Агенты «Аккорд-В.» в составе комплекса работают независимо от АРМ администратора безопасности информации (т.е. децентрализовано), что повышает уровень функционирования всей системы в целом, т.к. отсутствует «единая точка отказа» системы.

Адаптируемое решение

ПАК «Аккорд-В.» позволяет защищать виртуальные инфраструктуры дополненные различными подсистемами. Например, VDI (Horizon View, XenDesktop), антивирусы (Deep Security, Kaspersky Security для виртуальных сред) или средства резервирования (Acronis backup, Veeam backup).

ПАК «СЕГМЕНТ-В.»

Общие сведения

При проектировании системы безопасности виртуальной инфраструктуры архитектор сталкивается с рядом проблем, среди которых всегда присутствуют:

- **проблема «суперпользователя»** — то есть сосредоточение максимальных привилегий в рамках одной роли (пользователя). Для большинства систем такое

положение неприемлемо, Администратор безопасности информации (АБИ) должен иметь возможность ограничивать действия Администратора виртуальной инфраструктуры (АВИ): запрещать критичные для безопасности действия и разрешать некоторые только по согласованию, например, удаление виртуальной машины (нарушение целостности и доступности) или экспорт ее на диск (нарушение конфиденциальности).

- **проблема сегментирования —** то есть разбиения системы на сегменты и обеспечения их изоляции. Так как система может содержать различную информацию (иерархически категорируемую, то есть разного уровня секретности или неиерархически, то есть разного вида), может возникнуть ситуация, при которой она будет «перемешана». Например, случайное или умышленное переключение секретной ВМ в подсеть к несекретным или миграция ВМ разработчика на хранилище бухгалтерии.

К сожалению, данные проблемы не могут быть эффективно решены средствами самой виртуальной инфраструктуры. В итоге приходится подходить к вопросу «нестандартно», что ведет либо к дополнительным затратам, либо к снижению эффективности использования средств виртуализации, либо к введению дополнительных организационных мер усложняющих работу АБИ. По этой причине логичным шагом является перенимание опыта из смежных областей и использование наложенного средства защиты для ухода от описанных проблем.

Таким средством для виртуальных инфраструктур на базе VMware vSphere (версий 5.x и 6.x, для версии 6.5 поддержана работа с HTML5 клиентом) является программно-аппаратный комплекс «Сегмент-В.».

ПАК СЗИ НСД «Сегмент-В.» состоит из следующих компонентов:

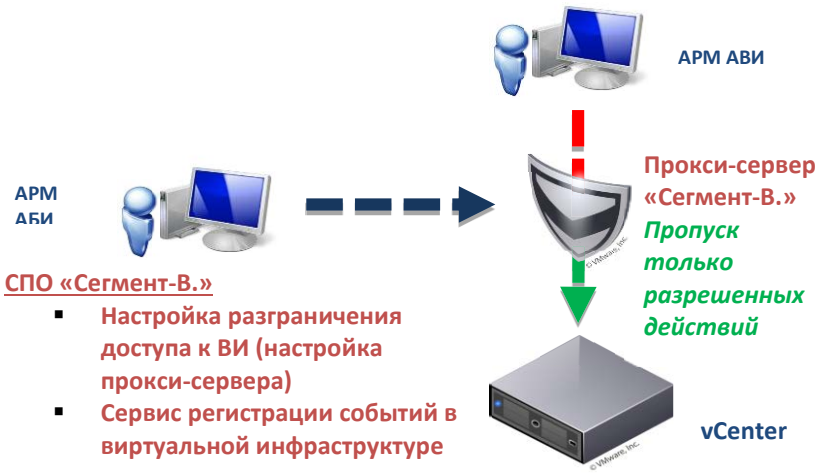
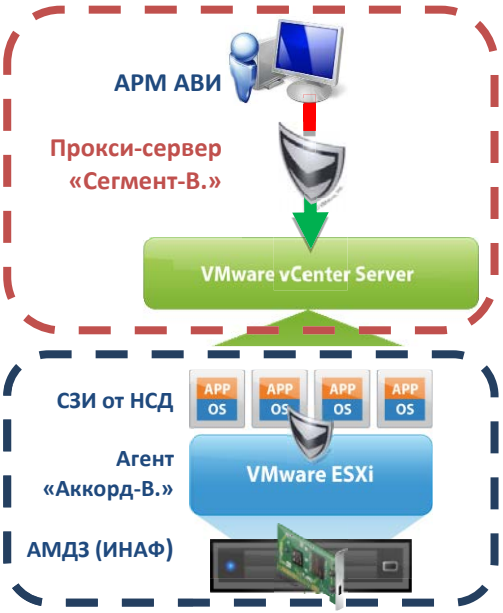


Схема взаимодействия

Прокси-сервер «Сегмент-В.» устанавливаемый в разрыв перед vCenter и осуществляющий разграничение доступа. Поставляется в трех вариантах:

- программном (.iso, подходящий для установки в ВМ);
- в виде функционального программно-технического комплекса (ФПТК) для установки на собственный сервер (включающий в себя кроме .iso также СЗИ НСД для защиты сервера);
- аппаратном (предварительно настроенный защищенный сервер, включающий «Аккорд-АМДЗ» и «Аккорд-Х», для которого достаточно провести первоначальную инициализацию).

СПО «Сегмент-В.» устанавливаемое на АРМ АБИ и включающее в себя ПО управления комплексом (сервис регистрации событий может быть установлен на отдельный АРМ).



Архитектура системы

ПАК «Сегмент-В.» может использоваться как самостоятельный продукт или в связке с ПАК «Аккорд-В.».

Возможности

В программно-аппаратном комплексе «Сегмент-В.» реализованы следующие механизмы защиты*:

- Идентификация/аутентификация пользователей управляющих виртуальной инфраструктурой
- Разграничение доступа к объектам виртуальной инфраструктуры:
  - Мандатное (иерархические и неиерархические метки)
  - Дискреционное (Более 20 действий)
- Запрет смешивания информации из различных сегментов

При этом система защиты:

- работает «прозрачно» (т.е. не требуется дополнительное ПО для работы АВИ)
- поддерживает отказоустойчивые кластерные конфигурации
- позволяет работать с любым вариантом инфраструктуры VMware vSphere (VCSA / Windows vCenter / Linked режим / Standalone ESXi).

Поэтому можно быть уверенным в том, что «Сегмент-В.» не ограничивает в целях безопасности возможностей виртуальной инфраструктуры, оставляя доступными все ее преимущества.

**Приведен список основных возможностей, с полным списком можно ознакомиться в документации на комплекс.*

Особенности

Выполнение требований регуляторов:

ПАК «Сегмент-В.» закрывает 5 из 10 требований (совместно с ПАК «Аккорд-В.» 7 из 10) по защите виртуальных инфраструктур (ВИ) приказов ФСТЭК № 17 и № 21:

- И/А в ВИ (ЗСВ.1)
- Управление доступом (ЗСВ.2)
- Регистрация событий (ЗСВ.3)
- Управление миграцией (ЗСВ.6)
- Сегментирование ВИ (ЗСВ.10)

Совместно с «Аккорд-В.»:

- Доверенная загрузка (ЗСВ.5)
- Контроль целостности (ЗСВ.7)

Исключения:*

- Управление потоками (ЗСВ.4)
- Резервирование (ЗСВ.8)

- Антивирусная защита (ЗСВ.9)

**закрываются представленными на рынке решениями*

Законченное решение

ПАК «Сегмент-В.» — самодостаточное решение. Требуется лишь настроить приобретенный сервер или «развернуть» новую ВМ. Отсутствуют скрытые затраты (например, на ОС).

Отказоустойчивое решение

ПАК «Сегмент-В.» поддерживает кластерную конфигурацию, что обеспечивает автоматическое переключение на резервный сервер в случае непредвиденных ситуаций.

Универсальное решение

ПАК «Сегмент-В.» поддерживает любые исполнения виртуальной инфраструктуры: VCSA / Linked Mode / Standalone ESXi. При этом решение не усложняет работу АВИ (отсутствуют какие-либо агенты).

ПАК «ГИПЕРАККОРД»

Общие сведения

ПАК «ГиперАккорд» предназначен для защиты инфраструктур виртуализации, построенных на базе платформ виртуализации Hyper-V версии 2 и версии 3.

Многие производители технических средств защиты инфраструктур виртуализации идут по пути универсализации, совмещая в своих продуктах механизмы защиты сразу нескольких инфраструктур, построенных на различных платформах виртуализации.

Однако данный подход не всегда удобен пользователям, когда в организации используются инфраструктуры виртуализации, построенные только на одном типе платформ, покупка так называемого «универсального» средства приводит, в частности, к следующим особенностям:

- наличие у средства избыточного функционала, часть которого никогда не будет использоваться на предприятии;

- удорожание средства защиты, влекущее за собой излишние расходы покупателя.

ПАК «ГиперАккорд» является специализированным средством для защиты инфраструктур виртуализации, построенных на платформе виртуализации Hyper-V, и, соответственно, лишен указанных недостатков.

ПАК «ГиперАккорд» состоит из следующих компонентов:

1. **СПО управления системой защиты «Гипер-Аккорд»**, устанавливаемое в ОС сервера HV, – является основным компонентом управления ПАК «ГиперАккорд», контролирует включение виртуальных машин и обеспечивает контроль целостности файлов внутри виртуальной машины до ее запуска. Данный модуль предоставляет также графический интерфейс, реализующий функции управления ПАК «ГиперАккорд»;
2. **ПАК для сервера управления** (ПАК «Аккорд-Win64 TSE»), устанавливаемый на сервере HV, в составе:
   - контроллер «Аккорд-АМДЗ», предназначенный для обеспечения доверенной загрузки ОС, установленной на сервере HV. Контроллер «Аккорд-АМДЗ» является универсальным, не требует замены при смене используемого типа ОС
   - персональный идентификатор пользователя – микропроцессорное устройство DS 199x («Touch memory») или ПИ ШИПКА. Используется для идентификации / аутентификации администратора безопасности информации и администратора виртуальной инфраструктуры на сервере HV;
   - съемник информации с контактным устройством, подключаемый в штатный USB-порт сервера HV сервера HV, обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя. По умолчанию в комплекте предлагается считыватель без фиксатора, если требуется с фиксатором – при заказе это нужно указать;
   - специальное ПО разграничения доступа «Аккорд-Win64 TSE», предназначенное для разграничения доступа к

ресурсам сервера HV со стороны администратора безопасности информации и администратора виртуальной инфраструктуры.

3. **СПО разграничения доступа для виртуальных машин** «Аккорд-Win32 VE»/ «Аккорд-Win64 VE»/ «Аккорд-X VE»/ «Аккорд-XL VE» (в зависимости от установленной в виртуальную машину ОС), предназначенное для разграничения доступа пользователей к ресурсам виртуальной машины, а также, в случае необходимости, для удаленного подключения к виртуальной машине с клиентских рабочих мест. Включает в себя:

- ПО «Аккорд ТС» (VE), устанавливаемое в ОС виртуальной машины;
- ПО «Аккорд ТК», устанавливаемое в ОС клиентских рабочих мест.

По умолчанию в качестве идентификаторов в процессе работы с ПАК «ГиперАккорд» предлагается использовать ТМ-идентификаторы.

Если в дальнейшем планируется использовать в качестве идентификатора не ТМ, а ПИ ШИПКА (на базе ШИПКА-лайт или других моделей), то никаких дополнительных кабелей для этого не потребуется, ПИ ШИПКА можно будет подключать напрямую в USB-порт, или через USB-удлинитель, если свободный USB-порт расположен неудобно.

Количество и тип идентификаторов, модификация контроллера и контактного устройства съемника информации оговариваются при заказе комплекса.

Возможности

В ПАК «ГиперАккорд» реализованы следующие механизмы защиты:

- доверенная загрузка всех элементов инфраструктуры виртуализации;
- пошаговый контроль целостности гипервизора, виртуальных машин, файлов внутри виртуальных машин и сервера управления инфраструктурой;

- разграничение доступа администраторов виртуальной инфраструктуры и администраторов безопасности;
- разграничение доступа пользователей внутри виртуальных машин;
- аппаратная идентификация всех пользователей и администраторов инфраструктуры виртуализации.

Защита клиентских рабочих мест

Для защиты клиентских рабочих мест требуется обеспечивать:

- доверенную загрузку установленной на клиентском месте операционной системы;
- разграничение прав доступа пользователей.

Средства защиты клиентских рабочих мест можно приобрести по дополнительному заказу:

1. для ПЭВМ:
- ПАК «Аккорд-Win32» в составе:
  - контроллер «Аккорд-АМДЗ»;
  - специальное ПО разграничения доступа «Аккорд-Win32»;
- ПАК «Аккорд-Win64» в составе:
  - контроллер «Аккорд-АМДЗ;
  - специальное ПО разграничения доступа «Аккорд-Win64»;

2. для тонких клиентов:
- ПАК «Центр-Т»;
- СОДС «МАРШ!»,

или защищенные СВТ для использования в качестве клиентских рабочих мест (микрокомпьютеры линейки МКТ, Ноутбук Руководителя).

Особенности

ПАК «ГиперАккорд» полностью интегрируется в инфраструктуру виртуализации, поэтому для его функционирования не требуются дополнительные серверы.

При этом ПАК «ГиперАккорд» не ограничивает в целях безопасности возможностей инфраструктуры виртуализации, оставляя доступными все ее преимущества и обеспечивая защищенность всех ее компонентов.

Управление системой защиты осуществляется централизованно с сервера управления виртуальной инфраструктурой. Доступ к инструментам управления системой защиты предоставляется только администраторам безопасности, от администраторов виртуальной инфраструктуры эти инструменты скрыты.

СПО «АККОРД-KVM»

Общие сведения

СПО «Аккорд-KVM» применяется для защиты виртуальных инфраструктур, построенных на базе KVM и использующих библиотеку libvirt (версии не ниже 1.2.8) в качестве инструмента управления гипервизором.

Основные защитные функции «Аккорд-KVM» базируются на

- контроле целостности программных компонентов ВМ (файлов общего, прикладного ПО и данных), выполняемом до их запуска;
- контроле целостности конфигурации ВМ, выполняемом до запуска ВМ;
- управлении размещением и перемещением исполняемых виртуальных машин между серверами виртуализации;
- регистрации событий безопасности в виртуальной инфраструктуре.

Возможности

В СПО «Аккорд-KVM» реализованы следующие механизмы защиты информации в инфраструктуре виртуализации[2]:

[2] Формулировки приведены согласно Методическому документу ФСТЭК России «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11 февраля 2014 года).

1. Регистрация событий безопасности в виртуальной инфраструктуре (ЗСВ.3).

2. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (ЗСВ.6). Управляющим персоналом комплекса обеспечивается управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных, включая

- управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных) в части контроля целостности конфигурации виртуальных машин;
- управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации в части обеспечения возможности разрешения или запрета запуска виртуальной машины на заданном хосте;
- управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных) в части контроля целостности конфигурации виртуальных машин.

При этом с помощью функции разрешения или запрета запуска виртуальной машины на заданном хосте можно обеспечить:

- полный запрет перемещения виртуальных машин (контейнеров);
- ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
- ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

3. Контроль целостности виртуальной инфраструктуры и ее конфигураций (ЗСВ.7), включающий в себя контроль целостности виртуальных машин, а также системных и пользовательских файлов внутри ВМ.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ПРИ УДАЛЕННОЙ РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ

ПАК «ЦЕНТР-Т»

Общие сведения

ПАК «Центр-Т» предназначен для обеспечения защищенной загрузки образов ПО (ОС) терминальных станций по сети.

Такая организация загрузки ПО терминальных станций позволяет контролировать его целостность и аутентичность, а также обеспечивать оперативное администрирование состава образа.

Казалось бы, к защите информации имеет отношение только целостность и аутентичность, так как контроль этих параметров позволяет обеспечить на терминале доверенную среду и создать предпосылки[3] для создания непрерывной защиты терминальной системы.

Однако администрирование состава образов тоже имеет самое прямое отношение к управлению правами пользователя системы. Ведь перечень доступных ему периферийных устройств, разрешение или запрет на флешки и токены, даже перечень доступных ему для подключения терминальных серверов – все это определяется в первую очередь именно составом образа ОС терминальной станции. То есть, например, запретив пользователю флешки на уровне ОС терминала, можно уже не задавать ограничений этого рода в ПРД для его учетной записи на терминальном сервере.

ПАК «Центр-Т» полностью реализован на специальных носителях информации (и клиентские, и серверные

[3] Речь может идти только о предпосылках потому, что ПАК «Центр-Т», подобно «Аккорду-АМДЗ» – обеспечивает только правильный старт, и дальше должен быть поддержан средствами защиты, функционирующими на следующих этапах. Поэтому в рекомендациях по условиям применения комплекса указано использование в системах терминального доступа или виртуальных инфраструктурах, защищенных СЗИ НСД «Аккорд TSE» или «Аккорд-В.».

компоненты размещаются на дисках, встроенных в эти устройства и могут исполняться на любом ПК), что обеспечивает комплексу значительную аппаратную независимость[4].

ПАК «Центр-Т» состоит из трех архитектурных компонентов:

- Автоматизированное рабочее место «Центр» (АРМ «Центр») – начиная с версии 1.2.0.1, применяется только для обеспечения обратной совместимости со старыми версиями, при разворачивании с нуля – не требуется;
- Сервер хранения и сетевой загрузки (СХСЗ);
- Клиентские устройства для терминальных станций.

Эти архитектурные компоненты реализованы на следующих аппаратных и программных.

Аппаратные компоненты:

- носитель ПО АРМ «Центр»;
- носитель ПО СХСЗ;
- носитель ПО Клиента;

Программные компоненты:

- ПО АРМ «Центр», размещенное в памяти носителя ПО АРМ «Центр» и исполняемое локально;
- ПО СХСЗ, состоящее из:
  - ПО сервисного режима работы СХСЗ, размещенного в памяти носителя ПО СХСЗ, доступ к которому предоставляется локально;
  - ПО управления СХСЗ, размещенного в памяти носителя ПО СХСЗ, доступ к которому

[4] В отдельных случаях по тем или иным причинам совместимость Центр-Т с СВТ не может быть обеспечена или требует совместных работ с вендорами СВТ. На сайте www.proTerminaly.ru систематически публикуются результаты проверок совместимости продукта с СВТ. Проведение проверки бесплатно при условии предоставления интересующей модели для проведения работ. Выдача сертификата совместимости на СВТ – платная.

предоставляется удаленно с АРМ Администратора и АРМ Администратора ИБ СХСЗ;

- ПО Клиента, размещенное в памяти клиентского устройства и исполняемое локально.

Для управления комплексом предусмотрены следующие роли.

На АРМ «Центр» – Администратор АРМ «Центр»;

На СХСЗ:

- Администратор сервисного режима работы СХСЗ (только локальный доступ);
- Администратор СХСЗ (только удаленный доступ);
- Администратор ИБ СХСЗ (только удаленный доступ);

На Клиенте:

- Пользователь;
- Администратор;
- Администратор ИБ.

Функции некоторых ролей могут выполняться одним сотрудником. Такими ролями являются:

- Администратор СХСЗ и Администратор клиентского устройства;
- Администратор ИБ СХСЗ и Администратор ИБ клиентского устройства;
- Администратор СХСЗ и Администратор сервисного режима работы СХСЗ.

Возможности

Схема работы выглядит следующим образом:

- со встроенного flash-диска носителя ПО СХСЗ стартует ПО СХСЗ. На момент начала эксплуатации он содержит предварительно подготовленные образы операционной системы (ОС) Linux, содержащие все необходимое ПО для соединения с терминальным сервером;

- с носителя ПО Клиента (далее также – клиентское устройство) стартует образ начальной загрузки (ОНЗ), также реализованный на основе ОС Linux. Далее на СХСЗ посылается запрос на получение образа с ПО ТС;
- СХСЗ обрабатывает запрос и выдает клиенту нужный образ ПО ТС;
- клиентское устройство принимает образ по сети и проверяет его. Если проверка образа завершается успешно, то он загружается в оперативную память СВТ и ему передается дальнейшее управление ресурсами компьютера;
- ПО, запущенное из полученного образа, инициирует соединение с терминальным сервером и осуществляет идентификацию пользователя на сервере.

Особенности

ПАК «Центр-Т» спроектирован таким образом, чтобы на пользователя клиентского устройства возлагался минимум дополнительных обязанностей, так как это роль сотрудника не IT или ИБ подразделений, задачи таких сотрудников состоят в выполнении операций, целевых для системы, а не в обеспечении ее работы. Поэтому функции пользователя клиентского устройства ПАК «Центр-Т» сводятся к следующим:

1. работа в рамках терминальной сессии;
2. изменение разрешения экрана;
3. просмотр сетевых настроек Клиента;
4. проверка работоспособности сети.

Все остальные функции как в отношении Клиента Центр-Т, так и в отношении СХСЗ, выполняются Администраторами.

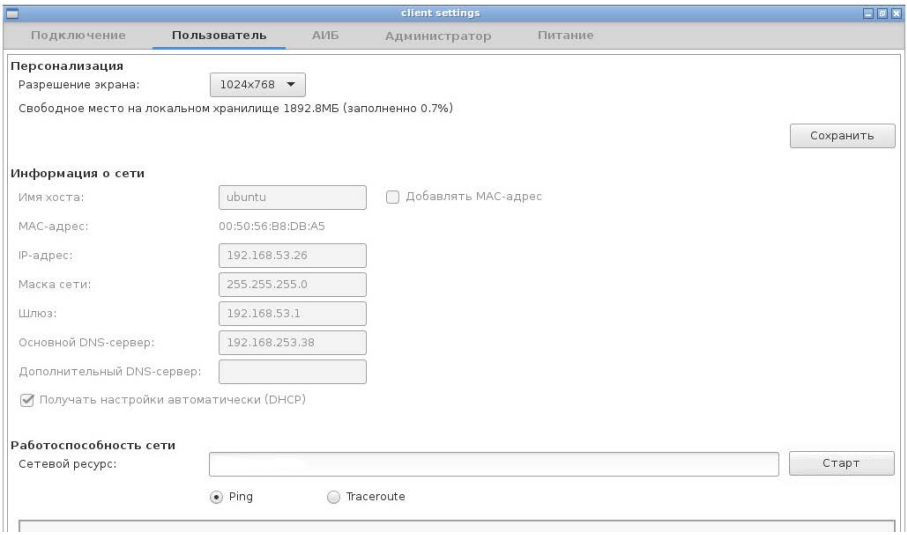
На Клиенте

Администратор клиентских устройств производит:

1. установку Пин-кода Администратора;
2. установку сетевых настроек Клиента;
3. смену Пин-кода Администратора.

Администратор БИ клиентских устройств производит:

1. установку Пин-кода Администратора БИ;
2. установку сетевых настроек для связи с СХСЗ;
3. смену Пин-кода Администратора БИ;
4. просмотр событий безопасности;
5. управление отладочным режимом.



Установка разрешения экрана

На СХСЗ

Функции СХСЗ в системе терминального доступа таковы:

1. управление учетными записями пользователей;
2. управление образами и шаблонами настроек образов ПО ТС;
3. предоставление образов клиентам (загрузка по сети).

Функции управления СХСЗ, начиная с версии 1.2.0.1, разделены между тремя административными ролями: Администратором сервисного режима, Администратором СХСЗ (далее также – Администратор) и Администратором БИ СХСЗ (далее также – Администратор БИ). Функции указанных ролей могут быть возложены на одно

должностное лицо, если это предусмотрено регламентирующими документами эксплуатирующей организации. Подробно с функциями этих ролей и возможностями комплекса можно ознакомиться в документе «Руководство по эксплуатации СХСЗ» из состава эксплуатационной документации на комплекс.

СОДС «МАРШ!»

Общие сведения

Коллективом ОКБ САПР разработана принципиально новая концепция: концепция доверенного сеанса связи удалённых пользователей с сервисами доверенной распределённой информационной системы через сеть Интернет, развивающая идеи доверенной вычислительной среды на основе резидентных компонентов безопасности.

Суть концепции состоит в предоставлении пользователю достаточных условий для защищённой работы с сервисами доверенной распределённой информационной системы не постоянно, а на определённый период времени, так как зачастую выполнение задач, требующих обеспечения доверенной среды, занимает незначительное время, а создание постоянной доверенной среды требует значительных средств и накладывает значительные ограничения.

Пользователи теперь могут работать на недоверенном компьютере в двух режимах: обычный режим (без доступа к сервисам доверенной распределённой информационной системы) и режим доверенного сеанса связи, в рамках которого обеспечивается защищённая работа с сервисами распределённой информационной системы. Выбор режима работы осуществляет пользователь. Это позволяет избежать ограничений, связанных с необходимостью специальным образом оборудовать компьютер пользователя и постоянно выполнять организационные требования, ограничивающие состав установленного ПО, права доступа, период работы и т.д. В нужное время пользователь может перейти в режим

ДСС и получить доступ к сервисам доверенной распределённой информационной системы. Закончив работу, он может вернуться в обычный режим и использовать компьютер без ограничений.

Таким образом, пользователи могут безопасно работать с сервисами доверенной распределённой информационной системы через сеть Интернет с любого, в т.ч. недоверенного компьютера.

Определение доверенного сеанса связи формулируется следующим образом.

Доверенный сеанс связи – период работы компьютера, в рамках которого обеспечивается доверенная загрузка ОС, организуется защищённое соединение, а также поддерживаются достаточные условия работы с электронной подписью.

Практической реализацией концепции доверенного сеанса связи является программно-аппаратный комплекс – средство обеспечения доверенного сеанса «МАРШ!».

СОДС «МАРШ!» предназначен для организации защищённой работы удалённых пользователей недоверенных компьютеров с сервисами доверенной распределенной информационной системы через сети передачи данных в рамках доверенного сеанса связи.

Комплекс СОДС «МАРШ!» состоит из клиентской и серверной части – Клиент доверенного сеанса связи и Сервер доверенного сеанса связи.

Клиент доверенного сеанса связи – загрузочное USB-устройство с собственным микропроцессором, который управляет доступом к нескольким аппаратно разделённым областям памяти на основании назначенных для них атрибутов. Устройство содержит загрузочную ОС, набор функционального ПО, средства защиты информации он несанкционированного доступа и средства криптографической защиты информации.

Сервер доверенного сеанса связи — доверенный сервер, обеспечивающий создание и работу защищённого сетевого соединения с пользователями, имеющими персональные устройства «МАРШ!» (Клиенты доверенного сеанса связи), с

целью предоставления им защищённого доступа к сервисам распределённой информационной системы.
Область применения комплекса:

- информационные системы Электронного правительства, государственных органов власти и органов местного самоуправления;
- распределенные защищенные информационные системы (например, органов внутренних дел) – доверенный доступ сотрудников;
- системы дистанционного банковского обслуживания;
- медицинские информационные системы;
- корпоративные системы обработки данных, содержащие персональные данные граждан.

Клиент СОДС «МАРШ!»

Возможности

Клиент доверенного сеанса связи может применяться в распределённой информационной системе в качестве:

- средства обеспечения доверенной загрузки ОС (ОС загружается из защищённой от записи памяти устройства, жёсткий диск компьютера не используется);
- средства обеспечения защищённого соединения с Сервером доверенного сеанса связи на основе асимметричных криптографических алгоритмов (закрытые ключи и сертификаты хранятся в защищённой памяти Клиента доверенного сеанса связи);
- средства идентификации \ аутентификации пользователя для доступа к сервисам распределенной информационной системы (в т. ч. хранение ключей и сертификатов);

- среды функционирования функционального ПО для подготовки и обработки данных;
- средства выработки и проверки электронной подписи данных;
- среды функционирования прикладного ПО сторонних производителей;
- средства хранения данных в выделенной области памяти устройства.

Сервер доверенного сеанса связи может применяться в распределённой информационной системе в качестве средства:

- организации защищённого соединения с Клиентом доверенного сеанса связи и Сервером авторизации распределённой информационной системы;
- авторизации пользователя Клиента доверенного сеанса связи на доступ к сервисам распределённой информационной системы;
- организации защищённой работы Клиента доверенного сеанса связи с сервисами распределённой информационной системы в рамках доверенного сеанса связи.

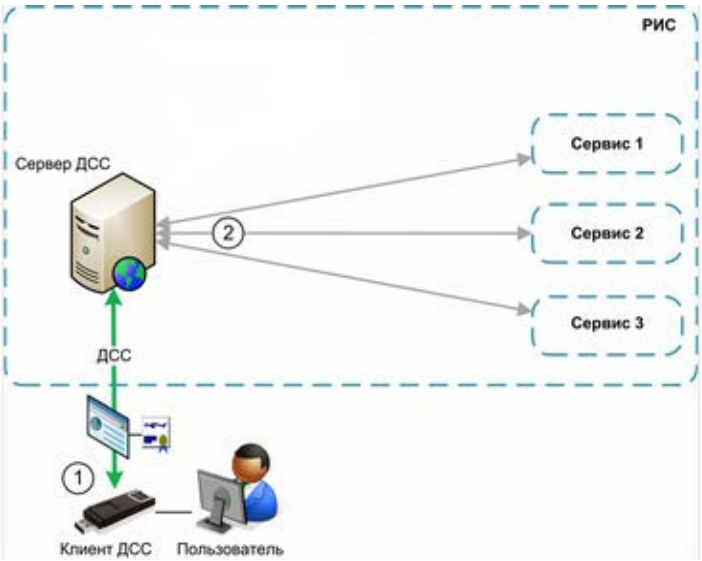


Схема работы СОДС «МАРШ!»

Схема работы СОДС «МАРШ!» выглядит следующим образом:

1. Удалённый пользователь недоверенного компьютера выполняет доверенную загрузку ОС с Клиента доверенного сеанса связи и устанавливает доверенный сеанса связи с Сервером доверенного сеанса связи.
2. Сервер доверенного сеанса связи выполняет авторизацию пользователя на доступ к сервисам распределённой информационной системы с помощью Сервера авторизации распределённой информационной системы.
3. Сервер доверенного сеанса связи соединяет пользователя с требуемым сервисом распределённой информационной системы.

Особенности

СОДС «МАРШ!» обладает следующими преимуществами:

- пользователю предоставляется необходимый функционал и достаточный уровень защиты (близкий к уровню доверенного компьютера с набором сертифицированных ОС, средств защиты информации от НСД и средств криптографической защиты информации);
- стоимость СОДС «МАРШ!» значительно ниже стоимости оборудования рабочего места необходимым для реализации политики изолированной программной среды набором средств защиты;
- СОДС «МАРШ!» является мобильным загрузочным устройством, готовым к работе на любом недоверенном компьютере;
- СОДС «МАРШ!» не накладывает ограничений на работу пользователя с компьютером вне доверенного сеанса связи.

В настоящий момент СОДС «МАРШ!» выпускается в нескольких вариантах исполнения и применяется для организации защищённой работы пользователей с рядом государственных и других доверенных распределённых информационных систем.

МИКРОКОМПЬЮТЕРЫ С НОВОЙ ГАРВАРДСКОЙ АРХИТЕКТУРОЙ

Микрокомпьютеры разработаны на базе 4-х ядерного Cortex-A9 процессора, причем в его состав включен мощный видеоускоритель, позволяющий воспроизводить файлы FullHD.

Новая гарвардская архитектура – это инновационная российская разработка, обеспечивающая целостность критичных ресурсов за счет, в частности, размещения в защищенной от перезаписи памяти, физически (на уровне схемотехники) изолированной от памяти перезаписываемой. Подробное описание архитектуры с обоснованием ее защищенности приведено в статьях и патентах, а также на сайте www.trustedcloudcomputers.ru.

Компьютерами можно управлять с помощью проводных (USB) и беспроводных (2.4 Ghz, bluetooth) мышек, клавиатур и пультов.

Поддерживается работа с защищенными ключевыми носителями по протоколу CCID.

Компьютеры линейки различаются между собой (кроме сценариев применения, для которых они предназначены) следующим набором параметров:

- наличием/отсутствием Ethernet,
- количеством и параметрами портов USB,
- количеством портов HDMI,
- количеством дисков для размещения ОС (и, соответственно, ОС),
- наличием\отсутствием внешнего (доступного пользователю) переключателя режимов работы,
- энергопотреблением,
- размерами и весом,
- световой индикацией.

MKT-CARD И MKT-CARD LONG

Общие сведения

«MKT-card» и «MKT-card long» – это доверенный облачный микрокомпьютер с динамически изменяемой архитектурой.

Конструктивно он оформлен как док-станция с отчуждаемым компьютером.

Док-станция содержит 8 USB-портов, выход HDMI, сетевой разъем RJ-45, разъем питания.

Док-станция коммутируется с периферийным оборудованием через USB, с монитором через HDMI, с сетью – через RJ-45; возможно также использование WiFi при условии разрешения на его применение.

Активная часть компьютера размещается в отчуждаемом модуле небольшого размера, что позволяет хранить его в стандартном пенале для ключей.

Микрокомпьютеры «MKT-card» и «MKT-card long»

Возможности

При использовании «MKT-card» и «MKT-card long» обеспечиваются:

- идентификация и аутентификация пользователя на сервере (кроме того, опционально «MKT-card»/«MKT-card

long» может сам выполнять функции аппаратного идентификатора пользователя в комплексах семейства «Аккорд» на терминальном сервере);

- «вирусный иммунитет»;
- регистрация действий пользователя;
- доверенная загрузка ОС.

Особенности

Функциональное ПО включает терминальные клиенты RDP и PC-over-IP, что позволяет обеспечить работу в облачной или терминальной инфраструктуре.

Встроены также средства разграничения доступа («Аккорд-ТК»), средства защищенного терминального доступа («Центр-Т»), средства «проброски» токенов и других периферийных устройств (например, защищенных USB-накопителей «Секрет Особого Назначения») на удаленный рабочий стол.

Наличие собственной ОС и вычислительных ресурсов позволяет обеспечить низкую стоимость владения удаленным «облачным» рабочим столом любой необходимой производительности, высокую скорость и надежность загрузки, высокий уровень защищенности.

Обеспечение стабильности среды функционирования криптографии позволяет встраивать и применять любые сертифицированные средства криптографической защиты информации.

- Защищенный диск: 1
- Размер диска: 8 ГБ

Параметры док-станции:

- Порт HDMI: 2
- Порт USB: 8 (host) + 1 (slave)
- Порт Ethernet: 1
- Порт питания: 1 DC 4.0mm
- Питание: DC 5V, 2A.

Размеры и вес защищенных терминалов:

Размер МКТ-card
1) в сборе – 9 (с учетом антенны WiFi — 10) x 9 x 3 см
2) отчуждаемый ПК – 9 x 5.5 x 1.3 см
Вес МКТ-card
1) в сборе – 164 гр.
2) отчуждаемый ПК – 50 гр.

Размер МКТ-card long
1) в сборе – 12 (с учетом антенны WiFi — 13) x 6.4 x 2.6 см
2) отчуждаемый ПК – 12 x 3.8 x 1.3 см
Вес МКТ-card long
1) в сборе – 160 гр.
2) отчуждаемый ПК – 49 гр.

M-TRUST

Общие сведения

Мезонин m-TrusT

m-TrusT – это одноплатный компьютер Новой гарвардской архитектуры, с общим назначением –защищенная сетевая коммуникация между элементами критической информационной инфраструктуры (КИИ).

Согласно 187-ФЗ[5] и его подзаконным актам, объекты КИИ (автоматизированные и информационные системы в их составе) подлежат защите также, как ГИС и ИСПДн высоких классов защищенности. В то же время у этих систем есть очень существенные отличия от систем «офисного типа», которые учитывает конструкция m-TrusT.

[5] Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Особенности

Конструктивно этот компьютер включает в себя док-станцию, которая стационарно включается в состав элемента КИИ, и подключаемого к ней универсального по своему аппаратному исполнению модуля – мезонина (m в названии микрокомпьютера – это именно «мезонин»).

Док-станция предназначена для того, чтобы корректно подключить m-Trust к тому или иному конкретному элементу КИИ, поэтому ее конструктивное решение и набор портов могут существенно различаться, ведь такими элементами могут быть самые разные объекты – от локомотивов до банкоматов, от газовых счетчиков до терминалов управления АЭС.

Это связано с тем, что самую высокую категорию значимости согласно Постановлению Правительства[6], будут иметь автоматизированные системы в составе объектов самого различного назначения, нарушение функционирования которых может привести к причинению ущерба жизни и здоровью более 500 человек (это, например, пассажирский поезд, средняя больница, вредное химическое производство) или нарушению условий жизнедеятельности (в том числе недоступность транспортных услуг и услуг сетей связи) более 5000 человек (например, несколько многоквартирных домов, крупный офисный центр, аэропорт).

Очевидно, что на таких объектах оборудование, защищенное сетевое взаимодействие которого нужно обеспечить, не просто имеет существенные особенности, но и является зачастую уникальным, то есть предъявляет жесткие требования к аппаратной адаптации средства защиты. Поэтому в случае, если не подходит ни один из ранее разработанных вариантов, док-станция проектируется для конкретного оборудования.

---

[6] Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Два типичные примера док-станции

Вариант 1 док-станции для m-TrusT

m-TrusT с док-станцией 1

- Габаритные размеры не более 90 х 105 мм
- Соединитель типа Розетка 87758-2016 MOLEX со следующими сигналами:
  - 1 контакт: +5 В
  - 3 контакт: USB D+
  - 5 контакт: USB D-
  - 7 контакт: Земля
  - 13 контакт: Ethernet RX-
  - 14 контакт: Ethernet TX-
  - 15 контакт: Ethernet RX+
  - 16 контакт: Ethernet TX+
  - 17 контакт: +5 В
  - 18 контакт: +5 В
  - 19 контакт: Земля
  - 20 контакт: Земля
- Разъем USB Type A
- Разъем Ethernet
- Ethernet скоммутирован через LAN-трансформатор PSF-16221 или аналогичный
- Разъем питания от источника постоянного напряжения 5 вольт

m-TrusT с док-станцией 2

Вариант 2 док-станции для m-TrusT

- Габаритные размеры не более 90 х 110 мм
- Соединитель типа Розетка 87758-2016 MOLEX со следующими сигналами:
  - 1 контакт: +5 В
  - 3 контакт: USB D+

- 5 контакт: USB D-
- 7 контакт: Земля
- 13 контакт: Ethernet RX-
- 14 контакт: Ethernet TX-
    - 15 контакт: Ethernet RX+
    - 16 контакт: Ethernet TX+
    - 17 контакт: +5 В
    - 18 контакт: +5 В
    - 19 контакт: Земля
    - 20 контакт: Земля
- USB-хаб
- Разъем USB Type A
- 2 разъема Ethernet
    - Один из разъемов Ethernet должен быть скоммутирован на Розетку через LAN-трансформатор PSF-16221 или аналогичный
    - Второй Ethernet-разъем должен быть подключен через преобразовать интерфейсов USB-Ethernet
- Разъем RS-232, подключенный через преобразователь USB-RS-232
- Разъем RS-485, подключенный через преобразователь USB-RS-485
- Разъем для micro-SD карты
- Разъем питания от источника постоянного напряжения 5 вольт

Возможности

В зависимости от того, что какие элементы КИИ должны взаимодействовать (подвижной состав и станционное оборудование, банкомат и АБС, какое-то измерительное оборудование и центр обработки (или центры агрегации) данных измерений, и т. д.) – ПО активной части m-TrusT, «мезонина» – будет разным. Оно создается для каждой конкретной задачи, поэтому Заказчиком приобретается не прибор, а *решение*, компонент именно той КИИ, для которой создается конкретная партия m-TrusT.

Например, это может быть проходной шифратор (прием данных и их передача в зашифрованном виде) или сбор и передача показаний каких-нибудь датчиков.

Функциональное программное обеспечение защищено вирусным иммунитетом Новой гарвардской архитектуры – оно загружается из памяти резидентного компонента безопасности (РКБ), которая защищена от вирусного заражения.

Съемный конструктив «мезонина» неоценимо упрощает обслуживание системы и ускоряет восстановление работоспособности при выходе «мезонина» из строя (что имеет огромное значение для КИИ) – он просто заменяется на новый путем подключения этого нового экземпляра к той же самой док-станции. Поскольку такой АРМ не хранит практически никаких данных, замена его рабочей части для системы не ощутима, если заранее сформирован некоторый фонд запасных устройств, обеспеченных нужными ключами и настройками.

TRUSTPAD

Общие сведения

«TrusTPad» – это планшет, построенный на новой гарвардской архитектуре по логике «МКTrusT».

Соответственно, в нем 3 раздела памяти, 2 ОС – защищенная и незащищенная, внутренний и внешний переключатели (режимов и ОС соответственно).

Возможности

- загрузка ОС в одном из режимов (защищенный и незащищенный);
- в защищенном режиме:
  - доверенная загрузка ОС;
  - «вирусный иммунитет»;
  - идентификация и аутентификация пользователя;

- поддержка защищенных USB-накопителей «Секрет Особого Назначения»;
- регистрация действий пользователя.

Защищенный планшет «TrusTPad»

Особенности

По сути это два планшета (защищенный и незащищенный) в одном корпусе.

- Bluetooth: v3.0 HS
- ОЗУ: 1 ГБ DRR3
- Порт HDMI другого типа: Порт Mini HDMI: 1
- Дисплей: 10.1” , 1280*800, 16:9 IPS
- Тач-панель: 1
- GPS приемник: 1
- ГЛОНАСС приемник: 1
- G-сенсор: 1
- Фронтальная камера: 1 (0.3 MP)
- Тыловая камера: 1 (2.0 MP)
- Лампочка фонарика: 1
- Встроенный микрофон: 1
- Аудиовыход: 1 (3.5 mm)
- Встроенный динамик: 1
- Батарея: 1 (6800mAh)
- Защищенный диск: 1
- Размер диска: 8 ГБ
- Незащищенный диск: 1

- Размер диска: 8 ГБ
- Диск для обновлений: 1
- Размер диска: 8 ГБ
- Порт питания: 1 DC
- Питание: DC 5V, 2.5A
- Световой индикатор режима работы: 1 (зеленый цвет – защищенный режим, красный – незащищенный)
- Звуковой индикатор режима работы: 1 (доступен в защищенном режиме)
- Переключатель режима работы.

АВТОМАТИЗИРОВАННЫЕ РАБОЧИЕ МЕСТА, ПОСТРОЕННЫЕ НА ПЛАТФОРМЕ ОПИСАННЫХ СВТ И СЗИ

ПАК «НОУТБУК РУКОВОДИТЕЛЯ»

Общие сведения

ПАК «Ноутбук руководителя» предназначен для обеспечения защищенной работы удаленных пользователей с сервисами доверенной распределенной информационной системы через сеть Интернет в рамках доверенного сеанса связи.

Название комплекса выбрано не случайно: ПАК «Ноутбук руководителя» обладает сразу несколькими свойствами, актуальными для рабочего места руководителей:

- хорошие показатели производительности персонального компьютера;
- мобильность;
- обеспечение доверенного сеанса связи;
- простота применения.

Комплекс реализован на базе ноутбука, средства защиты информации уже встроены в него, поэтому это решение позволяет упростить процесс проектирования защищенной информационной системы.

Процессор	2-ядерный; 1.7 ГГц; типа Intel Core i3, Intel Core i5 или Intel Core i7
Видео	видеокарта Intel HD Graphics 4600
Аудио	2 динамика
ОЗУ	2 ГБ, 4 ГБ или 8 ГБ; 1,6 ГГц, DDR 3 SDRAM
Емкость накопителя	500 ГБ
Интерфейсы	2 разъема совместимых с USB 2.0; два разъема совместимых с USB 3.0; VGA, HDMI, RJ-45, разъем для док-станции, слот для Smart Card, кардридер SD, комбинированный аудиоразъем
Батарея	6-секционная литий-ионная 65 Втч

В состав ПАК «Ноутбук руководителя» входят:

- ноутбук с версией BIOS, поддерживающей возможность загрузки с внешних носителей информации, и встроенным считывателем для смарт-карт;
- две смарт-карты (смарт-карта Администратора и смарт-карта Пользователя);
- аппаратный компонент – карта расширения (expansion card) с интерфейсом PCI-Express, на которую установлено ПО «Ноутбук руководителя».

Аппаратный компонент ПАК «Ноутбук руководителя» выполняет следующие функции в защищенном режиме:

- доверенную загрузку ОС;
- регистрацию контролируемых событий в системном журнале, размещенном в энергонезависимой памяти контроллера.

ПАК «Ноутбук руководителя»

Возможности

В комплексе сохранены все преимущества мобильной рабочей станции, но при этом обеспечиваются:

- загрузка ОС в одном из режимов (защищенный и незащищенный);
- в защищенном режиме:
  - доверенная загрузка ОС;
  - авторизация пользователей по смарт-карте;
  - возможность загрузки профиля[7] пользователя с определенными настройками и данными;
  - регистрация контролируемых событий в системном журнале контроллера.

Особенности

В обычном режиме безопасность сетевых соединений не контролируется, действия пользователя не ограничены, а ОС загружается из памяти ноутбука.

[7] Профиль пользователя — набор сетевых настроек, определяющих доступное подключение в рамках защищенного режима. Пользователю может соответствовать несколько профилей, однако должен быть выбран только один в рамках сеанса работы.

При выборе защищенного режима ОС загружается из защищённой от записи памяти комплекса «Аккорд-АМДЗ», входящего в состав ПАК «Ноутбук руководителя»; жёсткий диск ноутбука не используется. Пользователю предоставляется изолированная среда, в которой единственным доступным соединением является соединение, разрешенное администратором.

Режим выбирается пользователем при включении ноутбука, когда загружается сервисная ОС из состава ПАК «Ноутбук руководителя», проверяющая наличие привязанной к ноутбуку смарт-карты пользователя в считывателе.

ДВУХКОНТУРНЫЙ МОНОБЛОК

Двухконтурный моноблок – это, собственно, моноблок, позволяющий пользователю работать в одной из двух защищенных ОС (в общем случае одна из них Windows, а вторая – Linux). ОС Windows загружается с жесткого диска моноблока. При работе в этом режиме пользователь может устанавливать любое ПО и инициировать любые подключения в рамках заданных для него правил разграничения доступа: в ОС установлен ПАК «Аккорд-Win64».

Двухконтурный моноблок

При запуске Двухконтурного моноблока во втором режиме ОС Linux загружается из защищен-ного от записи раздела памяти микрокомпьютера «МКТ-card long»», то есть не просто с другого жесткого диска, а с другого компьютера.

Принципиальное отличие этого решения от решений на

базе подключаемых носителей доверенной среды состоит в том, что он не мобилен, но при этом предоставляет пользователю две полнофункциональные среды, а не только защищенный доступ к некоторой системе, при этом работа в этих средах может вестись параллельно, а не последовательно, для переключения не требуется ни перезагрузка, ни смена сеанса, все процессы продолжаются в каждой ОС своим чередом.

То есть это решение, которое:

- использует все возможности полноценного ПК;
- обеспечивает полноценную одновременную работу пользователя в любом режиме (удаленного доступа или локальном);
- позволяет использовать любой из режимов в качестве основного;
- обеспечивает необходимый уровень безопасности информации в каждом из режимов;
- позволяет легко осуществлять переход от одного режима обработки данных к другому.

На базе такой конструкции может создаваться целая палитра решений в зависимости от задач, определенных при проектировании системы: при желании заказчика может быть реализован вариант исполнения, для которого оба режима работы подразумевают терминальное соединение или, наоборот, локальную обработку данных etc. Неизменной остается идея продукта, подразумевающая реализацию следующих принципов:

- возможность работы на одном СВТ одновременно (насколько позволяет использование общего монитора, клавиатуры и мыши) с одним из двух контуров безопасности, изолированных друг от друга;
- соответствие каждому из режимов работы собственной ОС: ОС первого режима доступна только для чтения и содержит ПО, предустановленное на эта производства, ОС второго – доступна для записи (следовательно, возможна

самостоятельная установка ПО пользователем) и содержит СЗИ;

- надежное обеспечение информационной безопасности в каждом из режимов работы при правильной настройке Двухконтурного моноблока.

Переключение между режимами выполняется посредством нажатия:

- кнопки переключения для смены экрана, расположенной на корпусе моноблока, и
- KVM-переключателя,

установленного внутрь моноблока, для передачи сигналов клавиатуры и мыши к текущей системе.

Кнопка переключения режимов

То, какие именно два режима будут реализованы в двухконтурном моноблоке, зависит от задач конкретной системы, это определяется на стадии проектирования и обсуждается на этапе заказа. Например, в одном из вариантов исполнения Двухконтурный моноблок предоставляет пользователю два режима на выбор:

- локальный режим обработки данных (используется ОС семейства Windows);
- терминальный режим обработки данных (используется ОС Linux).

В локальном режиме ОС загружается с жесткого диска моноблока. При работе в этом режиме пользователь может устанавливать любое ПО (в рамках назначенных ему прав) и инициировать любые подключения. В ОС установлен ПАК «Аккорд-Win64», и при необходимости выполнения контрольных процедур до или во время работы пользователя администратор может произвести соответствующую настройку комплекса.

При запуске Двухконтурного моноблока во втором режиме ОС загружается из защищенного от записи раздела памяти микрокомпьютера «МКТ-card long». При работе в этом режиме пользователю доступно только ПО для доступа к

терминальному серверу и дополнительное ПО, необходимое для работы в рамках терминальной сессии.

Обновление «МКТ-card long» возможно по специальной защищенной процедуре, поэтому при необходимости внесения изменений в проект системы и систему – защищенность «МКТ-card long» от изменений не станет к этому препятствием.

Технические характеристики

Состав	2 независимых вычислительных узла в едином корпусе с интегрированным экраном, общими для узлов клавиатурой и указателем типа «мышь»
Экран	IPS 23», разрешение 1920×1080, время отклика 4 мс, яркость 300 кандел, количество отображаемых цветов 16,7 млн., угол обзора 178*178 градусов, покрытие экрана матовое антибликовое
Порты и интерфейсы	Интегрированные интерфейсные порты для подключения клавиатуры и мышки с защитой от съема информации
Клавиатура	104 клавиши с русскими и латинскими символами различного цвета, имеет отдельную клавишу для смены раскладки (RUS/LAT), отдельную клавишу для переключения между вычислительными узлами комплекса, оснащена цветосветовым индикатором, информирующим об отображаемом на экране комплекса вычислительном узле
Датчик вскрытия	Комплекс оснащен датчиком вскрытия, функционирующим как во включенном, так и в выключенном состоянии, фиксирующим факт вскрытия, выдающим сервисное сообщение о факте вскрытия и блокирующим

	дальнейшую работу комплекса при следующем после вскрытия включении
Идентификация и аутенти-фикация	Применяются аппаратные USB-идентификаторы, в комплект поставки входят два аппаратных USB-идентификатора ПСОМ ШИПКА-лайт Slim
Размер (в, Ш, г)	550 мм, 370 мм, 60 мм
Вес	6 кг

Технические характеристики вычислительного узла 1

Процессор	Intel® Core™ i3/i5/i7
Оперативная память	8, 16 или 32 Гбайт одноканальная стандарта DDR4 или 4, 8 или 16 Гбайт двухканальная стандарта DDR4
Дисковая подсистема	Твердотельные диски от 60 до 200 Гбайт или жесткие диски от 500 до 4000 Гбайт
Видеокамера	Интегрированная 2МП камера с механической шторкой
Порты и интерфейсы	2 x USB 2.0, 1 x USB 3.0, HDMI, Display Port, интегрированный считыватель смарт-карт, сетевой интерфейс RJ-45 1 Гигабит/сек
ОС	Astra Linux Special Edition, Альт Линукс СПТ 6.0/7.0, Windows 7 SP1 32 или 64 бит, Windows 10, в том числе сертифицированные во ФСТЭК

Технические характеристики вычислительного узла 2

Процессор	ARM Cortex A9 1,6 ГГц, четыре ядра, четыре потока, кэш-память 512 Кбайт
Оперативная память	2 Гбайт стандарта DDR3

Дисковая подсистема	8 Гбайт в режиме «Только для чтения», обеспечена целостность (неизменность) образа предустановленной операционной системы на аппаратном уровне
Порты и интерфейсы	Сетевой интерфейс RJ-45 100 Мбит/сек, возможна установка внешнего считывателя смарт-карт
ОС	Linux Ubuntu 12

КРИПТОМАРШРУТИЗАТОРЫ КМ И КМ SERVER

Общие сведения

Криптомаршрутизаторы КМ и КМ Server – полнофункциональное решение для построения VPN-сетей на основе протоколов SSLv3/TLSv1, с помощью которого можно решить широкий круг задач по обеспечению безопасного обмена информацией, включая подключение удаленных пользователей к корпоративной сети, безопасную связь между удаленными офисами, решения для удаленного доступа масштаба предприятий с поддержкой балансировки нагрузки, отказоустойчивости и четко разграниченным контролем доступа.

Комплекс обеспечивает криптографическую защиту информации (в соответствии с ГОСТ 28147–89), передаваемой по открытым каналам связи, между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры.

В качестве протокола транспортного уровня криптомаршрутизатор может использовать как TCP, так и UDP. Авторизация узлов может проводиться как на разделяемых ключах и шифровании трафика в режиме CFB, так и на сертификатах X509 и шифровании через SSLv3/TLSv1.

Особенности

Криптомаршрутизатор основан на Новой гарвардской архитектуре. Программное обеспечение размещено в памяти с физически устанавливаемым доступом read only (RO), что исключает искажения программного обеспечения и обеспечивает неизменность среды функционирования СКЗИ. Существует также возможность доверенного обновления ПО, что отличает данный криптомаршрутизатор от остальных решений на рынке.

Существует два варианта исполнения криптомаршрутизатора:

1. Исполнение 1 – VPN-сервер.
2. Исполнение 2 – VPN-сервер и сервер IP-телефонии – добавлен Voice over IP шлюз с 4 FXS портами и развернут сервер IP-телефонии. Такое решение позволяет осуществлять звонки между аналоговыми телефонами, подключенными к криптомаршрутизатору, и IP-телефонами, подключенными куда угодно. При этом трафик телефонов идет по VPN, а значит, защищен.

Исполнение 1 может быть выпущено в виде сервера в стойку и в виде микрокомпьютера MKT-card long.

Исполнение в виде микрокомпьютера называются KM Center (с серверными ключами) и KM Point (с клиентскими ключами), а исполнения в виде сервера – KM Center Server и KM Point Server, соответственно, и KM-Phone Center Server и KM-Phone Point Server – с IP-телефонией.

Возможна поддержка разных VPN-решений по требованию заказчика, так как не всегда удобна поддержка в одной организации разных ключевых систем.

Стоимость платформы (аппаратной части) криптомаршрутизатора на порядок ниже стоимости традиционных платформ с аналогичными вычислительными характеристиками и аналогичным уровнем защищенности. Учитывая

это, совокупная стоимость создания VPN-инфраструктуры обходится намного дешевле.

Характеристики аппаратной части сервера:

Характеристика	Исполнение 1	Исполнение 2
Форм-фактор	1U для монтажа в 19'' стойку либо микрокомпьютер MKT-card long	1U для монтажа в 19'' стойку
Габариты (ВхШхГ)		
Процессор	4-ядерный, 1,6 ГГц, Cortex A9	4-ядерный, 1,6 ГГц, Cortex A9
ОЗУ	2GB DRR3	2GB DRR3
Сетевые интерфейсы	4 порта Ethernet 100 Мбит/с	4 порта Ethernet 100 Мбит/с
Память	SD (TF card) до 32GB	SD (TF card) до 32GB
Порт HDMI	1	1
Порт USB	1	1
FXS порт	-	4

Характеристики программной части сервера:

Характеристика	Исполнение 1	Исполнение 2
ОС	ОС Linux собственной сборки	ОС Linux собственной сборки
VPN-сервер (СКЗИ)	ПК «LirVPN» (КС1 и КС2) (разработчик – ООО «ЛИССИ-Софт»)	ПК «LirVPN» (КС1 и КС2) (разработчик – ООО «ЛИССИ-Софт»)
Сервер IP-телефонии	-	Есть

Характеристика	Исполнение 1	Исполнение 2
Доверенное обновление ПО	Есть	Есть

Возможно централизованное управление стандартизированным средством управления R-Vision (то есть можно управлять одновременно и другими криптомаршрутизаторами, если в системе применяется несколько видов).

Количество портов от 1 до много, но суммарная пропускная способность по всем одновременно (если одновременно несколько пользователей «сидят» на разных каналах) – не выше 240 мегабит в сумме на все порты.

Пропускная способность между двумя портами – 80 мегабит (при использовании ГОСТ шифрования LirVPN).

ЗАЩИЩЕННЫЙ ТЕРМИНАЛ НА БАЗЕ «МКТ-CARD LONG»

Защищенный терминал – это один из основных типов АРМ на основе «МКТ-card long». Мы выделяем четыре основных типа терминала, построенных на базе этого микрокомпьютера, в каждом из которых есть специфические варианты реализации в зависимости от задач системы Заказчика.

Вне зависимости от варианта исполнения защищенного терминала на базе «МКТ-card long» и режима работы, после включения микрокомпьютера загружается его локальная ОС. ОС «МКТ-card long» размещена в памяти, доступной только для чтения (read only, RO), что исключает возможность её несанкционированного изменения, обеспечивает доверенную загрузку ОС, и, как следствие, неизменность среды исполнения функционального ПО. Память «МКТ-card long» защищена от записи на аппаратном уровне.

Варианты реализации защищенного терминала на базе «МКТ-card long» различаются способом организации хранения и загрузки ОС с использованием этой архитектурной особенности.

1. Базовый вариант — ОС полностью хранится в памяти RO микрокомпьютера и загружается локально. ОС содержит терминальный клиент (RDP или ICA — в зависимости от заказа) и клиент Аккорд TSE (Аккорд-ТК), а также может содержать другое функциональное ПО в соответствии с требованиями Заказчика.

2. Второй вариант локальной загрузки отличается тем, что конфигурационная информация, которая потенциально нуждается в изменении, выделяется из основного образа ОС и выносится на sd-карту, которая устанавливается в отчуждаемый компьютер из состава «МКТ-card long».

3. Однако может быть необходимость разделить ОС и иначе, выделив в переменную часть не только конфигурации, но и некий набор функционального ПО, в том числе и терминальный клиент, и что-то еще, что может потребовать изменения, и потому не может располагаться в неизменяемой памяти. В этом случае загружаться переменная часть образа ОС может по технологии защищенной сетевой загрузки, применяемой в ПАК «Центр-Т», с контролем целостности и аутентичности образа, загружаемого с СХСЗ. Такой вариант реализации защищенного терминала называется «МКТ-card long с поддержкой технологии Центр-Т».

После загрузки на микрокомпьютер функционального ПО и проверки его подлинности устанавливается соединение с терминальным сервером, производится идентификация и аутентификация пользователя на сервере с использованием аппаратного идентификатора ПИ ШИПКА (опционально «МКТ-card long» может сам выполнять функции аппаратного идентификатора пользователя). По завершении данной операции запускается терминальный клиент, и пользователь может приступить к работе в терминальной сессии. В рамках терминальной сессии пользователю может быть предоставлена возможность использования USB-устройств, подключенных непосредственно к «МКТ-card long».

4. Для систем, в которых с одного АРМ пользователю нужно получать доступ в два разных контура, разделенных

по функциональному принципу или по уровню защищенности, но так или иначе, изолированных один от другого, реализован вариант защищенного терминала «двойного назначения». В этом случае на этапе загрузки неизменяемой части ОС из защищенной памяти «МКТ-card long» пользователь выбирает, в какой контур ему нужен доступ в данный момент, и, в зависимости от этого выбора загружается одна или другая переменная часть ОС из одного или другого источника (с sd-карты, с СХСЗ или из RO памяти микрокомпьютера, в зависимости от заказа). Такой вариант реализации защищенного терминала называется «МКТ-card long для двойного применения».

Защищенность технологии доступа к терминальному серверу с использованием «МКТ-card long» обеспечивается:

- Технологически — за счет размещения ОС и встроенных средств защиты информации от несанкционированного доступа в защищенной от перезаписи памяти,
- технически — за счет применения СЗИ НСД и двухфакторной идентификации с применением аппаратного отчуждаемого персонального идентификатора (каковым может являться как дополнительное устройство (ТМ-идентификатор, ПИ ШИПКА, так и отчуждаемая часть терминала),
- организационно — отчуждаемый ПК из состава терминала после окончания работы может запираться пользователем в сейфе, сдаваться под охрану или сохраняться под персональную ответственность иным способом.

Удаленный доступ с защищенного терминала на базе «МКТ-card long» может осуществляться с помощью встроенных средств, выбранных на этапе заказа:

- клиента, обеспечивающего работу с фермой Citrix (Citrix Receiver);
- VMware Horizon Client;
- или Free RDP.

При использовании «МКТ-card long» во всех перечисленных вариантах обеспечиваются:

- идентификация и аутентификация пользователя на сервере;
- регистрация действий пользователя, в том числе, в отношении использования USB-устройств;
- целостность загружаемой ОС и защита от несанкционированной модификации программ и данных;
- поддержка применения в рамках терминальной сессии защищенных USB-носителей «Секрет Особого Назначения»;
- возможность применения токенов CCID, в том числе, поддерживающих технологию «привязки» к разрешенной рабочей среде («Идеальный токен»).

Защищенный терминал на базе «МКТ-card long» имеет ряд преимуществ перед решениями на базе традиционных аппаратных терминалов, поскольку его использование позволяет:

- снизить влияние на состояние системы фактора поддержки периферийного оборудования операционной системой терминального клиента;
- повысить защищенность информации за счет схемотехнической защиты от несанкционированной (в том числе, случайной) перезаписи и/или повреждения операционной системы терминального клиента (применения Новой гарвардской архитектуры компьютера);
- повысить эффективность организационных мер обеспечения защиты информации за счет возможностей аппаратной архитектуры;
- снизить стоимость комплекта «аппаратный терминал + средства обеспечения его защищенной загрузки»;
- упростить процесс администрирования системы за счет возможности унификации клиентских рабочих мест.

СХСЗ НА БАЗЕ «МКТ-CARD LONG»

Сервер хранения и сетевой загрузки (СХСЗ) описан в разделе, посвященном ПАК «Центр-Т». ПО СХСЗ размещено в классическом варианте исполнения на специальном USB-устройстве и исполняется на сервере, устанавливаемом в стойку в серверной комнате.

Однако мы предлагаем и другой вариант исполнения СХСЗ – на базе «МКТ-card long». Это решение так и называется СХСЗ на базе «МКТ-card long».

На этапе производства в защищенную от перезаписи память «МКТ-card long» может быть установлено ПО разного назначения, в том числе и ПО сервера хранения и загрузки ПО ТС по сети.

СХСЗ на базе «МКТ-card long» имеет следующие преимущества по сравнению с решением на базе традиционного сервера:

- низкая стоимость;
- техническая защита от модификации ПО сервера.

При этом сохраняются достаточно высокие вычислительные характеристики.

Рассмотрим типовые ситуации, в которых предпочтителен выбор решения, реализующего первый или второй подход.

Главное и очевидное отличие этих двух решений, определяющее положительные и отрицательный стороны применения каждого из них в конкретных условиях эксплуатации, — используемая аппаратная база.

Для применения решения на базе USB-устройства требуется дополнительное СВТ. Что очень важно, это СВТ должно быть совместимо со специальным встроенным ПО USB-носителя СХСЗ. В случае необходимости технической поддержки серверного компонента системы эксплуатирующая организация будет вынуждена обратиться к производителю СВТ — в одних случаях, к производителю решения для развертывания СХСЗ — в других. При разработке СХСЗ на базе «МКТ-card long» производитель решения несет ответственность за совместимость

программных и аппаратных компонентов, а обслуживание сервера выполняется одной организацией. Если решение для СХСЗ на базе USB-устройства приобретается одновременно с необходимым для его эксплуатации СВТ, то стоимость такого комплекта будет выше стоимости СХСЗ на базе «МКТ-card long». При этом если для СХСЗ используется СВТ из компьютерного парка организации (в том числе устаревший компьютер), общая стоимость развертывания СХСЗ может быть ниже стоимости решения на базе «МКТ-card long».

«МКТ-card long» имеет размеры 13×6.4×2.6 см. СВТ с подключенным USB-носителем, на базе которого реализован СХСЗ из состава ПАК «Центр-Т», очевидно, будет занимать больше пространства (возможно, значительно больше). Компактный размер «МКТ-card long» позволяет устанавливать его в телекоммуникационный шкаф. При этом никакие компоненты СХСЗ не будут выступать за пределы корпуса. Кроме того, имеется возможность изготовления СХСЗ на базе «МКТ-card long» в форм-факторе 1U для установки в стойку.

В случае если актуальными являются угрозы, связанные с загрузкой серверного ПО с внешних носителей, в организации, планирующей применение СХСЗ, может быть принято решение о запрете такого режима загрузки сервера в принципе. В этом случае применение решения для СХСЗ на базе USB-устройства становится невозможным. Выбор СХСЗ на базе «МКТ-card long» позволит развернуть сервер сетевой загрузки с необходимым функционалом и при этом соответствовать предъявленному требованию.

Различия между вариантами реализации СХСЗ сведены в таблицу.

Параметр сравнения	**Решение**		
	СХСЗ на базе USB-устройства	**СХСЗ на базе «МКТ-card long»**	**Примечание**

Габариты	Полноразмерный сервер в стойку + USB-устройство	Компактный	Габариты решения имеют значение в том случае, если есть особенности размещения СХСЗ
Стоимость	≈4700 $	≈780 $	Общая стоимость разворачивания СХСЗ на базе USB-устройства складывается из стоимости носителя с ПО СХСЗ и стоимости СВТ с учетом амортизации
Способ загрузки ПО	Загрузка с внешнего носителя	Загрузка из памяти микрокомпьютера	Способ загрузки ПО имеет значение в том случае, если загрузка сервера с внешнего носителя запрещена

Таким образом, СХСЗ на базе «МКТ-card long» может рассматриваться как предпочтительный вариант, когда:

- производится проектирование или модернизация системы терминального доступа;
- имеет значение размер оборудования (например, предполагается установка СХСЗ в телекоммуникационный шкаф);
- нет возможности выделения отдельного СВТ для развертывания СХСЗ;
- желательно упрощение технической поддержки оборудования;
- запрещена загрузка сервера сетевой загрузки с внешнего носителя.

Соответственно, выбор СХСЗ на базе USB-устройства может быть предпочтительнее, когда:

- для развертывания СХСЗ предполагается использование СВТ из компьютерного парка организации;
- габаритные размеры оборудования и порядок технической поддержки оборудования не имеют значения;
- загрузка сервера сетевой загрузки с внешнего носителя не запрещена.

Стоит отметить, что разные варианты исполнения могут использоваться совместно (например, при резервировании СХСЗ) и являются взаимозаменяемыми.

СИСТЕМА УДАЛЕННОГО ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «АККОРД» (СУЦУ)

Общие сведения

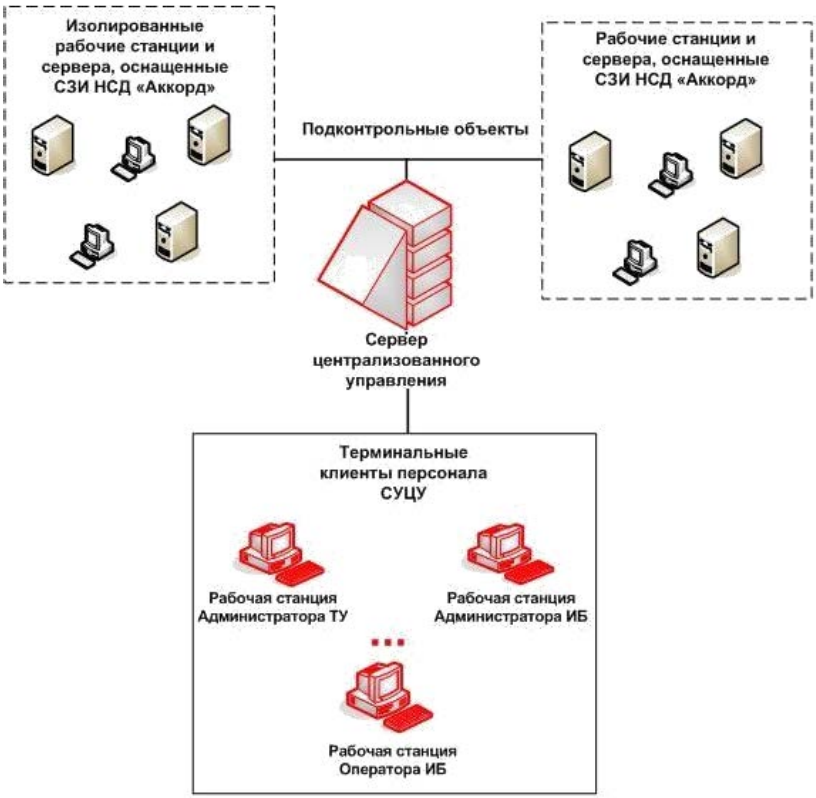
Система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд» предназначена для централизованного мониторинга событий информационной безопасности и управления средствами защиты информации от НСД.

Основные элементы СУЦУ:

- сервер централизованного управления (сервер централизованного управления – сервер терминального доступа, с помощью которого персонал СУЦУ может работать с ПО СУЦУ);
- подконтрольные объекты (рабочие станции и сервера, на которых установлены и функционируют средства защиты информации от несанкционированного доступа).

Возможности

- централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам;
- возможность централизованного управления средствами защиты информации от несанкционированного доступа на подконтрольных объектах;
- единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей.



Основные элементы СУЦУ

Управление техническими средствами:

- создание, редактирование и удаление технологического участка;
- редактирование состава рабочих станций и серверов технологического участка.

Управление пользователями:

- создание, удаление, редактирование учетных записей персонала СУЦУ;
- просмотр базы данных пользователей и ролей подконтрольных объектов;
- просмотр списка пользователей подконтрольных объектов технологического участка;

- создание, удаление, редактирование учетных записей пользователей технологического участка;
- создание, удаление, редактирование ролей пользователей;
- получение файлов конфигурации с выбранного подконтрольного объекта;
- редактирование и замену файлов конфигурации выбранного подконтрольного объекта;
- редактирование базы пользователей подконтрольных объектов на сервере централизованного управления:
- удаление пользователей подконтрольных объектов или изменение настроек их полномочий;
- добавление новых пользователей подконтрольных объектов и назначение им полномочий;
- синхронизация баз пользователей на подконтрольных объектах (в том числе, находящиеся в контроллерах) сразу после изменения базы или в момент начала работы подконтрольного объекта;
- передача изменений баз пользователей подконтрольных объектов;
- получение изменений баз пользователей от подконтрольных объектов.

Централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам:

- фиксирование и хранение информации о событиях информационной безопасности на подконтрольных объектах (фиксирование фактов изменения подконтрольного программного обеспечения, подключения / отключения устройств, подключения / отключения съемных носителей, регистрация для фиксируемых событий ИБ время выполнения действий, имя компьютера и имя пользователя);
- получение журналов подсистемы разграничения доступа с подконтрольных объектов;
- осуществление очистки журналов регистрации;
- систематизировано по соответствующим каталогам с делением по датам сбора.

Централизованное управление средствами защиты информации от несанкционированного доступа на подконтрольных объектах:

- механизм контроля целостности программного обеспечения подконтрольных объектов.

Управление списком зарегистрированных подконтрольных объектов:

- добавление, удаление и редактирование списка подконтрольных объектов на сервере централизованного управления СУЦУ;
- передача обновленного списка на подконтрольные объекты.

Управление доступом к коммутационным портам и периферийным устройствам:

- настройка доступа к периферийным устройствам;
- настройка доступа к коммутационным портам;
- создание единой базы «белых» и «черных» съемных носителей.

Особенности

Состав ролей СУЦУ:

- Администратор СУЦУ средств защиты информации от несанкционированного доступа: обеспечивает общее функционирование СУЦУ;
- Администратор информационной безопасности СУЦУ средств защиты информации от несанкционированного доступа: обеспечивает информационную безопасность в части защиты от несанкционированного доступа к ресурсам, включая контроль доступа к коммуникационным портам, рабочих станций и серверов подконтрольных объектов;
- Оператор СУЦУ средств защиты информации от несанкционированного доступа: обеспечивает мониторинг за функционированием системно-технической части СУЦУ;
- Оператор информационной безопасности СУЦУ средств защиты информации от несанкционированного

доступа: обеспечивает мониторинг состояния информационной безопасности в части защиты от несанкционированного доступа средствами СУЦУ и контроль событий безопасности информации, запротоколированных на подконтрольных объектах;

- Администратор информационной безопасности средств защиты информации от несанкционированного доступа (Администратор информационной безопасности технологического участка): обеспечивает информационную безопасность, в рамках полномочий, делегированных Администратором информационной безопасности СУЦУ;
- Администратор нештатного режима функционирования СУЦУ средств защиты информации от несанкционированного доступа: обеспечивает восстановление функционирования СУЦУ и подконтрольных объектов.

СРЕДСТВА ЗАЩИТЫ ДАННЫХ НА СЪЕМНЫХ НОСИТЕЛЯХ

ПАК «СЕКРЕТ ФИРМЫ»

Общие сведения

ПАК «Секрет фирмы» – это корпоративное решение, включающее в себя помимо необходимого числа специальных носителей пользователей также сервера аутентификации и регистрации.

При использовании этого комплекса работа со служебными носителями возможна только внутри корпоративной сети, причем для каждого носителя определяются те рабочие станции, которые разрешены для работы именно с ним. Особенность реализации комплекса позволяет оперативно прекратить работу с Секретами на всех компьютерах вообще, если это требуется в качестве реакции на какое-либо происшествие. Дополнительно можно установить режим запрета работы на всех или некоторых компьютерах с любыми другими USB-устройствами.

Идеально такое решение для сетей размером до 1000 абонентов на один сервер аутентификации.

В состав комплекса входят:

1. специальный носитель «Секрет Фирмы»;
2. два специальных носителя сервера аутентификации (СНСА) – эталонный и рабочий;
3. два специальных носителя эмитента – эталонный и рабочий;
4. ПО РС (нужно устанавливать на ПК, на которых планируется открывать «Секреты»);
5. ПО сервера аутентификации (нужно устанавливать на сервер аутентификации);
6. ПО эмиссии (нужно устанавливать на АРМ Эмиссии).

ПО РС, ПО сервера аутентификации и ПО эмиссии могут использоваться на РС типа IBM PC, функционирующих под управлением ОС Microsoft Windows, перечень конкретных версий ОС желательно уточнять, так как он постоянно расширяется. Кроме того, АРМ эмиссии и сервер аутентификации можно приобрести в сборе, в виде готовых АРМ «под ключ».

Возможности

ПАК «Секрет Фирмы» обеспечивает:

- кастомизацию служебных носителей для применения в рамках конкретной автоматизированной системы и нигде более;
- парольную аутентификацию пользователя;
- централизованное управление работой со служебными носителями;
- взаимную аутентификацию носителя информации и компьютерной системы;
- регистрацию действий пользователей и управляющего персонала системы.

Особенности

Использование «Секретов» на рабочих станциях корпоративной сети возможно при следующей совокупности условий:

1) Включен сервер аутентификации (СА) и к нему подключен СНСА.
2) На СА заданы правила, описывающие, какие «Секреты» можно использовать на каких компьютерах сети.
3) На компьютерах, на которых разрешено использование хотя бы одного «Секрета» установлено ПО РС.
4) «Секреты», эмитированные для данной организации и зарегистрированные на СА, используются в соответствии с разрешениями легальными пользователями, знающими PIN-коды.

На компьютере, не включенном в разрешенные, «Секрет Фирмы» не будет определяться как флеш-диск, поэтому сотрудникам не удастся использовать конфиденциальную информацию, хранящуюся в «Секрете Фирмы», на своем домашнем компьютере, или компьютере сети другой фирмы, даже если в той фирме тоже применяется технология «Секрет».

Для того чтобы исключить злоупотребления, основанные на сговоре администраторов, в комплекс включена система эмиссии. Служебные носители эмитируются в организации и для организации, ни разработчики, ни другая организация, использующая «Секреты», не сможет зарегистрировать чужой «Секрет» в своей системе и завладеть данными. При процедуре переэмитирования все данные будут стерты.

Для организаций, корпоративная сеть которых состоит из нескольких сегментов, предусмотрена возможность работы «Секрета» с разными СА одной сети, один из которых будет являться для этого носителя первичным, а остальные – вторичными, на работу с которыми первичный СА сможет выдавать своего рода «мандат».

Секрет

ПАК «СЕКРЕТ ОСОБОГО НАЗНАЧЕНИЯ»

Общие сведения

ПАК «Секрет Особого Назначения» (СОН) предназначен для сотрудников, в сферу ответственности которых входит работа с данным, конфиденциальность которых критична, но которые, вместе с тем, должны храниться на служебном носителе и переноситься сотрудником в рамках его должностных обязанностей на различные компьютеры.

То есть служебный носитель не должен использоваться бесконтрольно, но должен использоваться в том числе и на таких компьютерах, которые не администрируются управляющим персоналом организации и не входят в ее корпоративную сеть.

Очевидно, что это несколько противоречивые требования. Противоречие разрешимо, если все действия пользователя регистрируются в недоступном ему журнале. Этот механизм существенно повышает чувство ответственности пользователя, то есть может считаться не только защитной, но и воспитательной мерой.

Администратором может устанавливаться запрет на работу с СОНом на компьютерах вне заранее определенного перечня. Это удобно, если круг «чужих» компьютеров, на которых нужно работать с «Секретом», заранее определен и/или меняется не часто. Если запрет не установлен, то пользователь может подключать специальный носитель к «посторонним» для системы компьютерам – под свою персональную ответственность, так как информация об этом будет отражена в журнале.

Важно, что в журнале отображаются и удачные, и неудачные попытки подключения. То есть если даже диск «Секрета» не примонтировался, запись в журнале о том, что устройство для чего-то подключалось к неразрешенному компьютеру, останется.

В состав комплекса входят:

1. специальный носитель «Секрет Особого Назначения»;
2. ПО РС (не нужно устанавливать на ПК).

Важно, что ПО РС не требуется устанавливать на компьютер, оно загружается со встроенного диска СОНа и работает в оперативной памяти. То есть для работы с СОНом не требуются права администратора компьютера.

ПАК «Секрет Особого Назначения» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением ОС Microsoft Windows.

Возможности

ПАК «Секрет Особого Назначения» обеспечивает:

- парольную аутентификацию пользователя;
- разграничение доступа администратора и пользователя устройства к настройкам и журналу;
- взаимную аутентификацию носителя информации и компьютера;
- регистрацию действий пользователя.

Особенности

Диск СОНа имеет два раздела – открытый (но защищенный от записи) и защищенный (но доступный для записи после примонтирования).

Первый из них содержит ПО СОНа, которое может обновляться в специальном защищенном режиме. Защита от записи имеет целью предотвратить повреждение ПО.

Этот раздел монтируется при подключении устройства, как любая флешка, и стартующее с него ПО определяет соответствие или несоответствие компьютера параметрам тех, что находятся в списке разрешенных, и разрешает или запрещает монтирование. До принятия положительного решения о компьютере пароль пользователя не запрашивается.

Опознавание компьютера производится по совокупности следующих признаков:

1. Номер материнской платы компьютера,
2. ID операционной системы,
3. Серийный номер электронного замка («Аккорд» или «Соболь»),
4. Имя компьютера,
5. Идентификатор домена.

Особые модификации: Быстрый секрет и Секрет Руководителя

«Секрет Особого Назначения» реализован на базе криптографического Секрета, то есть с аппаратным шифрованием всех данных при записи на диск (и расшифровыванием при чтении). По заказу может быть изготовлена партия и без поддержки шифрования. При этом скорости чтения и записи данных с/на флеш-память указанных вариантов реализации следующие:

- Базовый СН: 5 МБ/с и 8.8 МБ/с;
- Криптографический СН: 200 КБ/с и чтение, и запись.

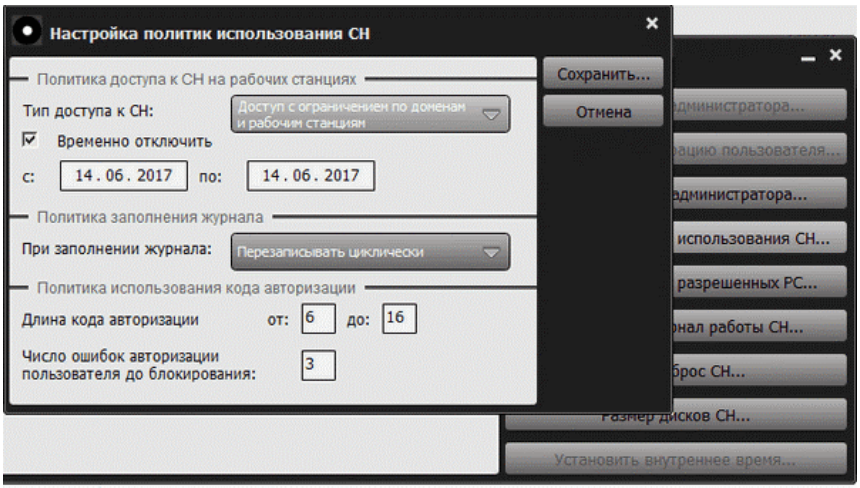
Предсказуемо, что скорость работы СН с шифрованием довольно мала – пользователю придется подождать при чтении и записи данных с/на флешку. Кого-то это совершенно не смущает, ведь главное – это защищенность данных (в условиях невысокой стоимости устройства), а другие готовы использовать СН без шифрования лишь бы только привычные действия выполнялись быстрее. Иногда компромисс неуместен, и для этих случаев есть отдельное решение – СОН на базе служебного носителя «Быстрый Секрет», его скорость заметно выше: 6.1 МБ/с (чтение) и 5.7 МБ/с (запись).

Объем диска всех перечисленных СН может быть 8/16/32 ГБ – этот параметр влияет на стоимость, поэтому дифференциация по нему тоже – вполне уместна.

Общаясь с представителями организаций, эксплуатирующих Секреты, мы обнаружили еще одну особенность. Действительно, не для всякого сотрудника уместен порядок, при котором для изменения режима доступа следует обратиться к администратору. Например, довольно неловкой для всех является ситуация, когда по окончании командировки руководитель должен сдать свой Секрет для установки запрета на подключение к посторонним машинам, снятого на период командировки под его ответственность. Более того, скорее всего, руководитель просто забудет об этом. А в установке этого запрета ведь заинтересован в первую очередь он сам, так как именно это гарантирует конфиденциальность данных в

случае потери или кражи устройства. Можно вменить руководителю обязанность самому администрировать свое устройство, тогда он сам сможет добавить новый ПК в разрешенные, а затем аннулировать регистрацию. Однако на руководителя, как правило, возлагается так много совершенно необходимых обязанностей, что от выполнения «лишних» действий он закономерно хочет быть избавлен. Для таких случаев мы сделали Секрет Особого Назначения на базе служебного носителя «Секрет Руководителя».

В Секрете Руководителя администратор может временно (на интервал дат) отключить все запреты и разрешить подключение к неограниченному кругу компьютеров.



Настройка политик доступа использования СН Секрет Руководителя

Это возможно без снижения защищенности за счет наличия встроенных часов реального времени (RTC) – подмена системного времени не обманет устройство. Через заданный период времени ограничения на подключение снова вступают в силу.

Обратная связь дает нам возможность учитывать особенности существования устройств в реальной жизни. В результате сейчас, выбирая служебный носитель, на базе которых реализован Секрет Особого Назначения, можно (и

нужно учесть): объем флешки, потребность в шифровании, скорость работы СН, потребность во временной установке и снятии ограничений.

USB-НАКОПИТЕЛЬ «ТРАНЗИТ»

Еще один пример продукта, возникшего на основе потребности нашего тогда еще будущего Заказчика – это USB-накопитель «Транзит» – флешка с неперезаписываемым внутренним ПО.

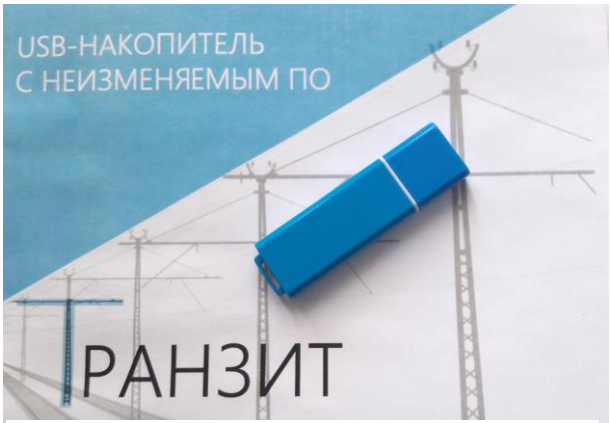
Иными словами – это флешка, которая не может стать ничем другим, так как ее нельзя перепрограммировать.

Осознание того, что даже самая простая флешка по сути является компьютером с собственным процессором и собственной памятью, привело к тому, что перепрограммированные USB-накопители стали считаться важными и весьма вероятными каналами утечки.

Известен целый класс атак, называемый BadUSB, в основе которого лежит модификация firmware USB-устройств для выполнения несанкционированных действий процессором этих самых USB-устройств. Кроме того, существуют варианты реализаций штатных протоколов взаимодействия USB-устройств с нештатными расширениями, которые могут быть использованы и как скрытые каналы управления, и как нелегальные хранилища для конфиденциальной информации (об этом есть много статей как в специальной литературе, так и на специальных форумах).

Эта уязвимость блокируется применением носителей, firmware которых защищено от перезаписи, например, специальных служебных носителей семейства «Секрет». Однако, у служебных носителей «Секрет» есть собственная функциональность (описанная выше), и если она в системе не требуется, то их применение избыточно. USB-накопитель «Транзит» не имеет никакой дополнительной функциональности, это именно флешка, но флешка, которую нельзя перепрограммировать, то есть такая, которая точно не сможет быть использована как-то кроме как по прямому назначению.

«Транзит» функционирует на ПЭВМ, поддерживающих работу устройств по интерфейсу USB. Для подключения к ПЭВМ двух или более носителей «Транзит» может использоваться USB-хаб. В этом случае USB-хаб должен быть оснащен внешним источником питания. Для корректной работы «Транзит» должны быть установлены драйверы носителя информации. Драйверы устанавливаются автоматически при первом подключении носителя «Транзит» к USB-порту.



Транзит

ПАК «ПАЖ»

Общие сведения

ПАЖ

Для мониторинга информационной безопасности должны обеспечиваться сбор и хранение журналов событий. В «ОКБ САПР» создали для этого специальный ПАК «ПАЖ» («Программно-аппаратный журнал») — средство ведения неперезаписываемого журнала событий, удобное в использовании и удовлетворяющее требованиям к защищенности такого рода информации.

ПАК «ПАЖ» включает:

1. специальный носитель «ПАЖ» — USB-флешка объёмом 8, 16 или 32 Гб для сбора и хранения журналов приложений, которая содержит в себе энергонезависимую флеш-память и собственный микроконтроллер;
2. ПО РС, которое содержится на открытом разделе флеш-диска специального носителя и не требует установки.

ПАК «ПАЖ» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением ОС семейства Windows.

Возможности

- экспорт файлов журналов событий различных приложений из заданного каталога на жестком диске компьютера на диск аппаратного неперезаписываемого журнала;
- экспорт журнала комплекса «Аккорд-АМДЗ» на диск аппаратного неперезаписываемого журнала;
- интеграция со сторонним программным обеспечением в части ведения аппаратного неперезаписываемого журнала с использованием специальной библиотеки, входящей в состав ПАК «ПАЖ» и реализующей интерфейс программирования приложений (API) для записи журналов приложений;
- задание правил доступа к содержимому аппаратного журнала посредством настройки соответствующих политик: работа с диском аппаратного журнала на чтение или запись возможна только на заранее зарегистрированных в качестве разрешенных СВТ. На любых других СВТ диск устройства не будет смонтирован, и оно не будет определяться в системе как «съемный диск». Все случаи подключений (как успешные, так и неуспешные) записываются в собственный журнал устройства, доступный для просмотра только его администратору.

Особенности

Функционирование компонентов ПАК «ПАЖ» обеспечивает управляющий персонал, реализующий роли пользователя, администратора, и аудитора:

- администратор: осуществляет настройку ПАЖ, включая управление ролями ПАЖ; контролирует использование специального носителя посредством проверки внутреннего журнала работы;
- пользователь: добавляет журналы приложений на специальный носитель. При этом журнал сохраняется в каталоге специального носителя, соответствующем рабочей станции, на которой происходит его добавление;
- аудитор: просматривает журналы приложений на специальном носителе.

ПАК «ИДЕАЛЬНЫЙ ТОКЕН»

Общие сведения

Специализированные средства хранения криптографической информации – токены – предоставляют возможность использования хранимых на них сертификатов и ключевой информации после предъявления PIN-кода (авторизации пользователя). Казалось бы, таким образом блокируются все уязвимости, связанные с нарушением свойств безопасности криптографической информации.

Однако токен как часть криптографического средства защиты, функционирует в некоторой среде, которая складывается из технических и программных средств, образующих среду функционирования криптографического средства и способных повлиять на выполнение им собственных функций. Использование технических и программных средств порождает объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы безопасности информации.

Очевидно, что ограничение доступа к ключу только использованием PIN-кода недостаточно. Токен должен

использоваться только в той системе, в которой обеспечена защита от несанкционированного доступа (а значит, обеспечена доверенная среда функционирования криптографического средства), а PIN-код можно правильно ввести в любой среде. Токен не может определить, в какой системе производится попытка работы с ним. Например, в этой системе могут быть предустановлены программные закладки, предназначенные для перехвата криптографической информации или перехвата управления компьютером. При правильно введенном PIN-коде (а в некоторых случаях и до введения PIN-кода) все это программное обеспечение получит доступ к ключам.

Один из способов гарантировать использование криптографической информации в пределах четко выделенной доверенной среды функционирования криптографического средства – ограничение числа компьютеров, на которых технически возможна работа с токеном. В случае реализации такой защитной меры при случайном или преднамеренном подключении токена к неразрешенному (а значит, недоверенному) компьютеру, устройство не будет примонтировано, значит, ключи не будут доступны ни пользователю (даже легальному), ни системе (с потенциально функционирующими в ней вирусами и закладками). Кроме того, исключено несанкционированное использование ключей легальным пользователем токена вне рамок его служебных задач.

Функции токена с функцией ограничения числа разрешенных компьютеров объединяет в себе новое средство, разработанное компанией ОКБ САПР, – «Идеальный токен».

«Идеальный токен» включает в себя USB-устройство со специальным встроенным программным обеспечением и специальное программное обеспечение, устанавливаемое на компьютер.

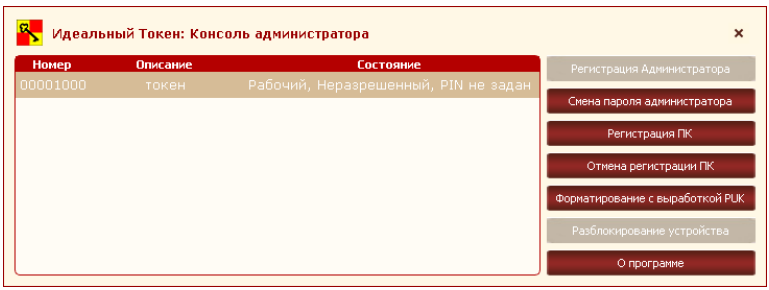
«Идеальный токен» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением операционных систем семейства Windows.

Возможности

Устройство «Идеальный токен» может использоваться в качестве хранилища ключей и сертификатов в том числе для средства криптографической защиты информации производства компании «КриптоПро», для системы криптографической авторизации электронных документов «Сигнатура».

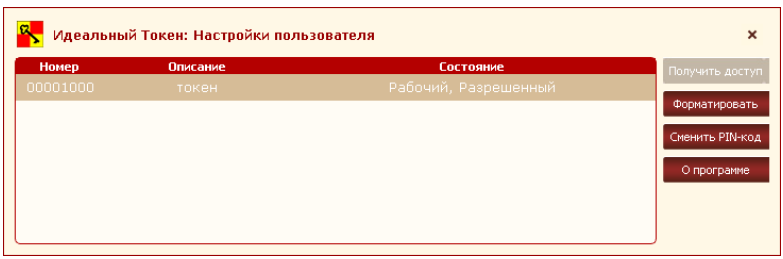
Особенности

Список компьютеров, на которых разрешена работа с «Идеальным токеном», определяется администратором информационной безопасности.



Главное окно утилиты «Консоль администратора»

При каждом последующем подключении устройством определяются параметры текущего компьютера и сравниваются с теми данными, которые были получены при добавлении компьютера в список разрешенных.



Главное окно утилиты «Настройки пользователя»

Если они совпадают, разрешается доступ к токену со стороны внешнего (по отношению к «Идеальному токену») ПО – то есть, собственно, со стороны средства криптографической защиты информации, иначе в доступе отказывается.

МОБИЛЬНЫЙ НОСИТЕЛЬ ЛИЦЕНЗИЙ

Лицензирование ПО – это очень тонкая и многогранная тема, и с защитой информации она связана как правило в разрезе защиты ПО от несанкционированного копирования, использования и распространения.

Одно из решений этой задачи предложено в разделе «Решения» на сайте www.okbsapr.ru, здесь же речь пойдет о решении задачи защищенного распространения лицензий.

Решение предназначено для тех, кто уже сделал выбор в пользу лицензирования с предоставлением пользователю ПО ключевой информации, необходимой для установки или активации ПО.

В этом случае с точки зрения продавца и покупателя могут возникать сложности и сомнения следующего рода.

Продавец:

- должен каким-то способом обеспечить невозможность многократного применения одной и той же лицензии, для этого она, как правило, формируется для конкретного рабочего места с учетом его уникальных характеристик;
- должен сделать процесс выработки и передачи лицензий таким, чтобы он не оказывал разрушающего влияния на процесс продажи, в котором зачастую задействованы третьи фирмы (интеграторы, дистрибьюторы), а характеристики рабочих мест, на которых будет применяться ПО, зачастую на момент покупки просто неизвестны.

Покупатель:

- не должен оплачивать один и тот же экземпляр ПО каждый раз при смене характеристик рабочего места (в случае, если лицензирование поэкземплярное);
- не должен передавать «наружу» характеристики информационной системы, если он считает целесообразным сохранять их конфиденциальность.

В общем случае для получения лицензии этого вида требуется предоставление уникальных идентификационных признаков рабочих станций (UID ОС компьютера или ВМ).

Самые распространенные трудности, связанные с этим процессом можно обобщить следующим образом:

1. организация может отказаться разглашать UID рабочих станций;
2. количество компьютеров, для которых необходима лицензия, может оказаться значительным, что увеличит время сбора необходимой информации;
3. при использовании технологии «золотого образа» в виртуальных инфраструктурах UID'ы ОС непостоянны.

На практике время сбора данных для лицензий может варьироваться от нескольких минут до нескольких дней.

Так, для исключения необходимости разглашать UID'ы, ОКБ САПР создана специальная утилита сбора лицензионных данных, которая формирует производные данные, не передавая в ОКБ САПР сами UID'ы. Для случая с «золотыми образами» сформирована инструкция, состоящая, вкратце, в том, чтобы задать диапазон UID'ов, из которого будет выбираться один произвольный при создании ВМ, и получить лицензионные ключи на весь диапазон. Все эти проблемы решаемы, но для каждой из них вырабатывается отдельное решение, и сочетание проблем требует сочетания решений, что еще больше запутывает процесс.

Кроме того, необходимость в получении лицензий может возникнуть внезапно, даже в выходной день. Конечно, в таких случаях можно найти (и находятся) возможные способы выхода из ситуации, однако не всегда результат достигается с желаемой скоростью.

Для решения большинства возможных сложностей, связанных с получением лицензий, разработан ПАК «Мобильный носитель лицензий» (МНЛ). ПАК «МНЛ» предназначен для распространения лицензий на лицензируемые изделия и состоит из:

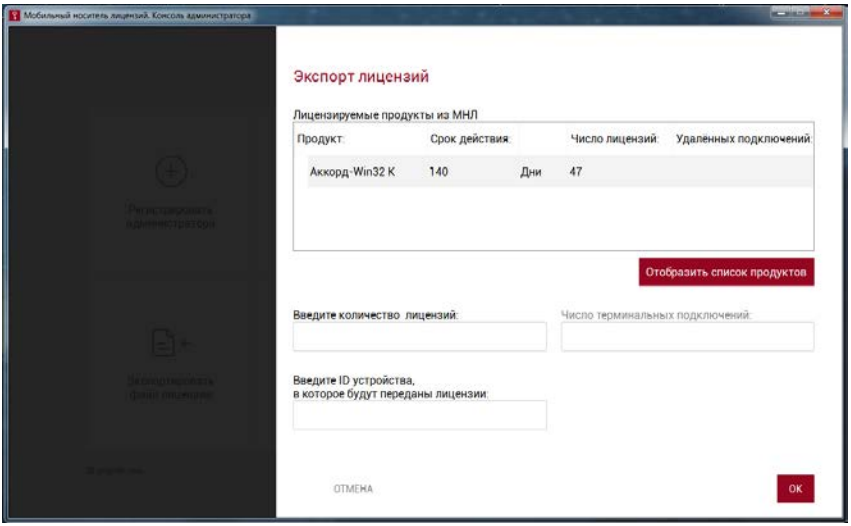
мнл

- аппаратного модуля МНЛ, который реализован как USB-устройство;
- специального ПО для управления лицензиями.

На устройстве МНЛ хранятся данные для генерации лицензий и счетчик доступных пользователю лицензий. Для генерации лицензии пользователь сам вводит запрашиваемые данные и указывает место сохранения файла лицензии. При необходимости файл лицензии может быть сгенерирован для удаленной рабочей станции. После генерации лицензии количество доступных лицензий снижается на единицу.

Стоит отметить, что ПАК «МНЛ» упрощает процесс получения лицензии за счет оптимизации процесса взаимодействия покупателя ПО с его продавцом, однако внедрение ПАК «МНЛ» косвенно положительно влияет и на скорость выполнения внутренних процессов, не нарушая их, так как никакой внутренней информации предоставлять никому не нужно: покупатель приобретает желаемое количество носителей и периодически запрашивает пополнение счетчика лицензий на тот или иной продукт по мере их расходования.

Важным обстоятельством является возможность передачи количества доступных лицензий с одного устройства на другое. Если возникнет необходимость контролировать расходование лицензионных ключей иерархически, пополнения счетчика могут запрашиваться на МНЛ головного подразделения организации – покупателя, а затем «раздаваться» на МНЛы других отделений.



Окно экспорта лицензий из одного МНЛ на другие

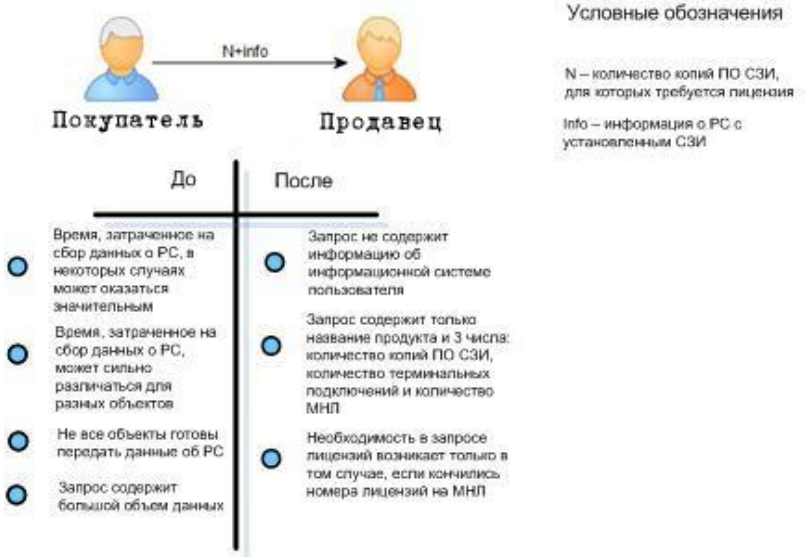
Эта же функциональность заметно упрощает работу через фирмы-посредники. Дистрибьютор (или системный интегратор) пополняет счетчик лицензий на общее число планируемых к реализации лицензий, а далее по мере формирования конкретных заказов, организует их распределение по МНЛ, которые будут входить в состав поставки покупателю, ведь одной организации будет достаточно одного МНЛ на всю поставку, а другой будет удобнее получить несколько – по числу территориальных подразделений, например.

Для организации более сложных схем работы с лицензионными ключами, предполагающими отзыв лицензий, например, в ОКБ САПР имеется проект сервера

лицензий, адаптируемый под потребности систем конкретных Заказчиков.

Таким образом, информация о компьютерной системе не покидает пределов эксплуатирующей ПО организации, и согласование возможности выдачи информации о РС, равно как и сам сбор информации о РС, не требуется. Это значительно (в ряде случае в несколько раз) уменьшает временные затраты на получение лицензий.

Особенности этапа обращения пользователя в ПТО до применения ПАК «МНЛ» и с применением ПАК «МНЛ» представлены на рисунке.



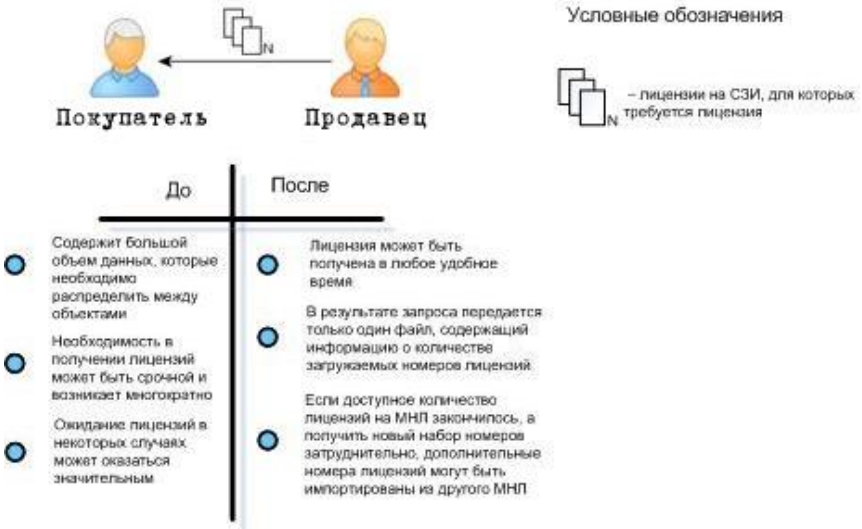
Особенности этапа обращения пользователя за лицензией

При условии применения ПАК «МНЛ» лицензия может быть сгенерирована самим пользователем в любое удобное время. Процедура проста и занимает минимум времени.

Если доступное количество номеров лицензий на устройстве из состава ПАК «МНЛ» закончилось, пользователю по запросу отправляется только один файл, содержащий необходимое количество номеров лицензий. В

случае если необходимость получения лицензии является срочной, но нет возможности получения нового набора номеров лицензий от производителя СЗИ, список номеров лицензий может быть экспортирован с другого МНЛ администратором устройства, а затем – импортирован пользователем или администратором в необходимый МНЛ. Или можно поступить иначе – сгенерировав лицензию для удаленной РС с помощью ПАК «МНЛ», на котором не закончились доступные номера лицензий.

Все особенности этапа получения лицензий до применения ПАК «МНЛ» и с применением ПАК «МНЛ» представлены на рисунке.



Особенности этапа получения лицензий

Как видно из приведенного описания, использование ПАК «МНЛ» значительно упрощает процесс получения лицензий на СЗИ, уменьшая объем затрачиваемых на выполнение процесса временных ресурсов и количество взаимодействующих при этом лиц. Это особенно ценно в случаях, когда лицензия на СЗИ требуется срочно или в конце рабочей недели.

При этом использование ПАК «МНЛ» не требует изменения установленных в организациях порядков выполнения внутренних процессов или выдачи сторонним организациям информации о компьютерных системах, использующих приобретаемое ПО.

СРЕДСТВА ИНТЕГРАЦИИ С СИСТЕМОЙ ВИДЕОМОНИТОРИНГА

УНИВЕРСАЛЬНЫЙ ХАБ «РАССВЕТ»

Общие сведения

Универсальный хаб «Рассвет» предназначен для:

- объединения подсистемы информационной безопасности и других подсистем информационной системы организации в интегрированную информационную систему;
- выделения информационных потоков взаимодействия компонентов интегрируемых подсистем в отдельную сеть, независимую от основной сети взаимодействия СВТ объекта информатизации.

Устройство «Рассвет» является периферийным устройством, подключаемым к USB-хосту контроллера ПАК «Аккорд-Win32» («Аккорд-Win64») или USB-хосту СВТ – подконтрольного объекта средств защиты информации от несанкционированного доступа. Подконтрольным объектом средств защиты информации от несанкционированного доступа является автоматизированное рабочее место под управлением ОС Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, оснащенный ПАК «Аккорд-Win32» («Аккорд-Win64»).

Возможности

С использованием устройства «Рассвет» могут быть обеспечены:

- интеграция на уровне персональных идентификаторов;
- выделение информационных потоков взаимодействия компонентов подсистем в отдельную сеть, независимую от

основной сети взаимодействия СВТ объекта информатизации, с возможностью их интеграции;

- дополнительная аутентификация пользователя по биометрическим данным (рисунку сосудистого русла ладони).

Особенности

Устройство «Рассвет» поддерживает возможность использования следующих видов идентификаторов пользователей:

- ТМ-идентификатор DS1991(2,3);
- ТМ-идентификатор DS1996;
- ШИПКА;
- карта Legic;
- карта ACOS3;
- карта HID;
- комбинированная карта.

В зависимости от того, использование каких идентификаторов и способов аутентификации определено проектными решениями на данном объекте информатизации, устройство «Рассвет» может использоваться совместно со следующими видами считывателей:

- считыватель ТМ-идентификатора с USB-разъемом;
- считыватель контактных смарт-карт;
- считыватель бесконтактных смарт-карт;
- считыватель сосудистого русла ладони встроенный в компьютерную мышь;
- комбинированный считыватель контактных смарт-карт и сосудистого русла ладони;
- комбинированный считыватель бесконтактных смарт-карт и сосудистого русла ладони.

КОМПЛЕКС ИНТЕГРАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С СИСТЕМОЙ ВИДЕОМОНИТОРИНГА И КОНТРОЛЯ ДОСТУПА «РАССВЕТ-СВМИКД»

Общие сведения

Комплекс интеграции СЗИ НСД с системой видеомониторинга и контроля доступа «Рассвет-СВМиКД» позволяет:

- выделить информационные потоки взаимодействия компонентов системы контроля управления доступом, видеомониторинга и средств защиты информации от несанкционированного доступа в отдельную сеть, независимую от основной сети взаимодействия средств вычислительной техники объекта информатизации;
- объединить подсистему информационной безопасности и систему контроля управления доступом в интегрированную систему видеомониторинга и контроля доступа к автоматизированным рабочим местам организации.

Комплекс «Рассвет-СВМиКД» устанавливается на подконтрольный объект – автоматизированное рабочее место под управлением ОС Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, оснащенный ПАК «Аккорд-Win32» («Аккорд-Win64»).

В состав комплекса «Рассвет-СВМиКД» входят:

- универсальный хаб «Рассвет»;
- устройство трансляции видеосигнала через сеть;
- сетевая видеокамера;
- комплект идентификаторов и считывателей.

Возможности

С использованием комплекса «Рассвет-СВМиКД» могут быть обеспечены:

- интеграция на уровне персональных идентификаторов;
- передача видеоданных с мониторов автоматизированных рабочих мест и с видеокамер на управляющие сервера системы контроля управления доступом без использования основной сети функциональной системы;
- выделение информационных потоков взаимодействия компонентов системы контроля управления доступом, видеомониторинга и СЗИ НСД в отдельную сеть, независимую от основной сети взаимодействия средств вычислительной техники объекта информатизации, с возможностью объединения ПИБ и СКУД в интегрированную систему видеомониторинга и контроля доступа к автоматизированным рабочим местам организации;
- дополнительная аутентификация пользователя по биометрическим данным (рисунку сосудистого русла ладони).

С использованием комплекса «Рассвет-СВМиКД» может быть обеспечено выполнение задачи видеонаблюдения за оператором, передачи для оперативного мониторинга видеопотока с экрана монитора и архивирования этого видеопотока на случай разбора инцидентов. Видеонаблюдение за оператором производится с помощью сетевой камеры, закрепленной на мониторе рабочего места или иным образом, и направленной на оператора. Передача видеопотока с экрана монитора производится с помощью устройства трансляции видеосигнала через сеть.

Особенности

В состав комплекса «Рассвет СВМиКД» по выбору Заказчика могут входить следующие комплекты идентификаторов и считывателей:

1. считыватель сосудистого русла ладони встроенный в компьютерную мышь и два ПИ ШИПКА на базе ШИПКА-лайт Slim;
2. считыватель ТМ-идентификатора с USB-разъемом, считыватель сосудистого русла ладони встроенный в компьютерную мышь и два ТМ-идентификатора DS1996;

3. считыватель контактных смарт-карт, считыватель сосудистого русла ладони встроенный в компьютерную мышь и две контактные смарт-карты;

4. считыватель бесконтактных смарт-карт, считыватель сосудистого русла ладони встроенный в компьютерную мышь и две бесконтактные смарт-карты;

5. комбинированный считыватель контактных смарт-карт и сосудистого русла ладони и две контактные смарт-карты;

6. комбинированный считыватель бесконтактных смарт-карт и сосудистого русла ладони и две бесконтактные смарт-карты.

СЕРВЕР ИНТЕГРАЦИИ СЗИ НСД И СИСТЕМЫ ВИДЕОМОНИТОРИНГА И КОНТРОЛЯ ДОСТУПА

Общие сведения

Сервер интеграции СЗИ НСД и системы видеомониторинга и контроля доступа является управляющим компонентом, обеспечивающим взаимодействие серверов СЗИ НСД и серверов СКУД в части интеграции на уровне объединения объектов доступа и логического взаимоувязывания помещений и компьютеров.

Сервер обеспечивает взаимодействие комплексов интеграции «Рассвет СВМиКД» и сервера системы видеомониторинга и контроля доступа, и представляет собой сервер в форм-факторе, допускающем возможность установки в серверную стойку 2U, под управлением 64-битных ОС Microsoft Windows Server 2008 R2 или Windows Server 2012, оснащенный ПАК «Аккорд-Win64 TSE».

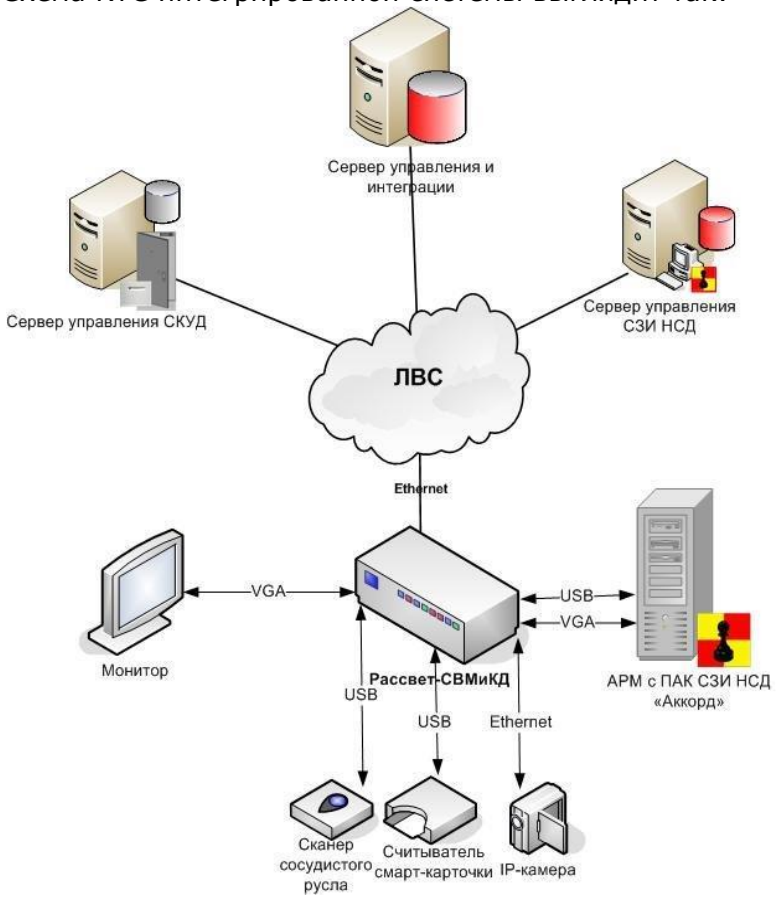
В общем случае предполагается поставка ПО для имеющегося в организации сервера, однако возможна поставка и сервера в сборе.

ПО Сервера поставляется на CD и содержит все компоненты, необходимые для выполнения функций Сервера интеграции средств защиты информации от несанкционированного доступа и системы видеомониторинга и контроля доступа, в том числе:

- серверные и клиентские компоненты, реализующие транспортные функции;
- серверные компоненты, реализующие функции интеграции серверов средств защиты информации от несанкционированного доступа и серверов системы контроля управления доступом.

Средства защиты информации от несанкционированного доступа серверов, серверов системы контроля управления доступом и подконтрольных объектов не входят в состав специального программного продукта Сервера интеграции.

Схема КТС интегрированной системы выглядит так:



Структурная схема интегрированной системы

Взаимодействие компонентов системы при этом выглядит так:

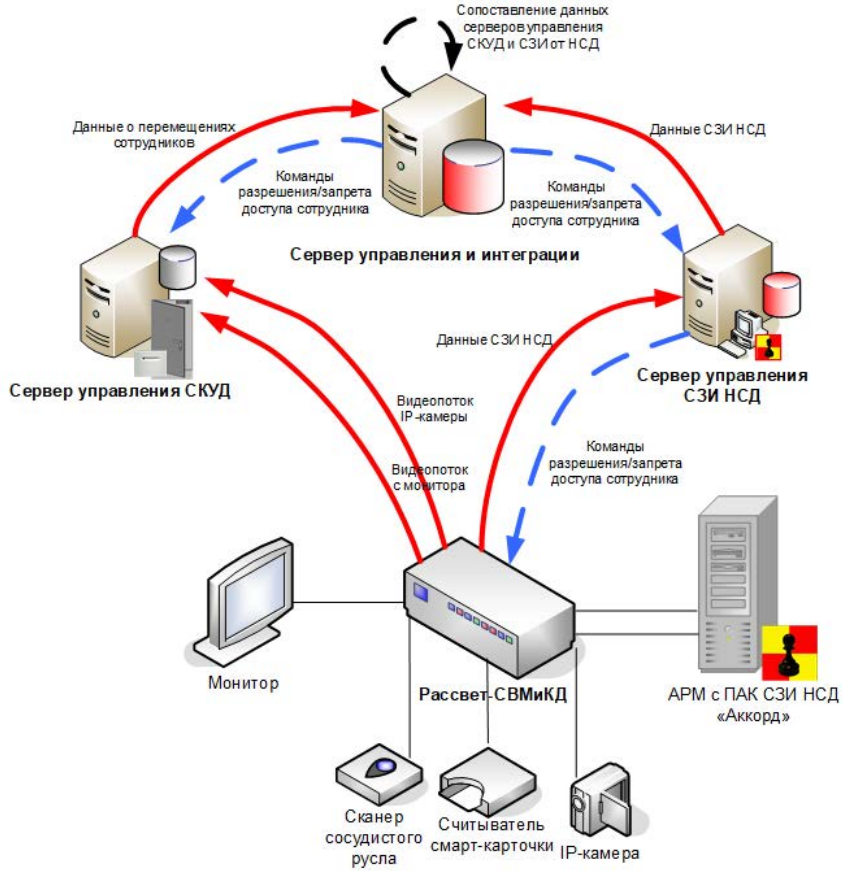


Схема информационных потоков интегрированной системы

Возможности

Применение Сервера позволяет создать новые правила доступа как к ПЭВМ, так и к помещениям, в целях повышения безопасности объекта информатизации. Частные наборы правил и условий их сочетаний вырабатываются для каждой системы отдельно управляющим персоналом системы.

Например, условием доступа к определенному автоматизированному рабочему месту может быть вход в определенное помещение, а условием выхода за пределы предприятия может быть отключение автоматизированного рабочего места (не выключив его, сотрудник не сможет покинуть периметр).

Особенности

В базовом варианте исполнения Сервер функционирует в автоматическом режиме, без поддержки ролевой структуры управляющего персонала организации. Однако, поскольку ПО Сервера всегда адаптируется под требования конкретной системы, оно может быть изменено и в части реализации таких ролей.

ИДЕНТИФИКАТОРЫ ПОЛЬЗОВАТЕЛЕЙ И СЧИТЫВАТЕЛИ ИДЕНТИФИЦИРУЮЩЕЙ И/ИЛИ АУТЕНТИФИЦИРУЮЩЕЙ ИНФОРМАЦИИ

АППАРАТНЫЕ ИДЕНТИФИКАТОРЫ

Одним из важнейших механизмов защиты информации от несанкционированного доступа является процедура идентификации пользователя.

Идентификация пользователя может осуществляться как программными механизмами (с использованием логина — последовательности символов, вводимых вручную с клавиатуры, позволяющей идентифицировать субъект), так и аппаратными (с использованием специального устройства, предоставляющего уникальный набор символов, позволяющий идентифицировать обладателя устройства).

Требования по реализации процедуры идентификации и аутентификации определяются руководящими документами в области защиты информации. При этом аппаратная идентификация/аутентификация относительно программной меры имеет статус дополнительной, усиливающей.

Например, утвержденный ФСТЭК России методический документ «Меры защиты информации в государственных информационных системах» предъявляет следующие требования к реализации меры защиты ИАФ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА:

«В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации — определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами…».

Одним из усилений данной меры защиты является следующее:

«В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ».

Очевидно, аппаратная реализация механизма идентификации в силу физической изолированности обеспечивает эффективную защиту от НСД наиболее важных процедур и данных, используемых при аутентификации в информационных системах.

Продукты, разработанные в «ОКБ САПР», поддерживают работу с аппаратными идентификаторами различных видов: TM-идентификаторы DS-1992, DS-1993, DS-1996, смарт-карты, USB-устройства, USB-ключи вида eToken, JaCarta «ACOSxx», «ESMART Token xx», считыватели биометрических данных и др.

Кроме того, для реализации механизма аппаратной идентификации в «ОКБ САПР» разработан ПАК «ПИ ШИПКА», обеспечивающий идентификацию пользователя в автоматизированных системах обработки данных путем реализации функции предоставления уникального номера USB-устройства «ПИ ШИПКА» по запросу.

ПАК «ПИ ШИПКА» может использоваться в качестве персонального идентификационного устройства при идентификации/аутентификации как в различных программных продуктах, так и программно-аппаратных изделиях и комплексах (например, СЗИ НСД «Аккорд-АМДЗ», ПАК СЗИ НСД «Аккорд»).

ПАК «ПИ ШИПКА» включает в себя:

- аппаратную базу — USB-устройство «ПИ ШИПКА»;
- встраиваемое программное обеспечение «ПИ ШИПКА»;

- программную надстройку — специальное программное обеспечение (СПО) «ПИ ШИПКА», устанавливаемое в ОС СВТ.

Для использования ПАК «ПИ ШИПКА» требуется следующий минимальный состав технических и программных средств:

- IBM-совместимый ПК, поддерживающий работу устройств по интерфейсу USB стандарта 1.1. или 2.0;
- установленная операционная система (семейства Windows (32-битная, 64-битная) или семейства Linux (32-битная)), поддерживающая спецификацию протокола обмена данными CCID Rev.1.1 посредством соответствующего системного CCID-драйвера;
- свободный разъем USB.

ПИ ШИПКА

БИОМЕТРИЧЕСКИЕ СЧИТЫВАТЕЛИ

В ПАК «Аккорд-Win32» и «Аккорд-Win64» поддержана аутентификация пользователя по сосудистому руслу ладони.

Решение интегрированное, использует сканеры сосудистого русла PalmSecure.

От классической версии комплекса данная комплектация отличается тем, что пользователь аутентифицируется не по паролю, вводимому с клавиатуры, а по биометрическому признаку: рисунку вен ладони или отпечатку пальцев. Опционально можно настроить необходимость дополнительного ввода пароля с клавиатуры.

Верификация пользователя производится путем сравнения предъявленной руки с эталоном, хранящимся в идентификаторе (ТМ 1996, ПИ ШИПКЕ, смарт-карте) пользователя в защищенном виде. Тем самым не создается база биометрических данных пользователей, сама в свою очередь нуждающаяся в защите. Положительный результат верификации обрабатывается комплексом «Аккорд» в качестве аутентифицирующих данных.

Считыватели предлагаются трех типов:

- совмещенный с манипулятором мышь сканер сосудистого русла, дополненным подставкой для удобства размещения руки над сканером (PalmSecure). После прохождения верификации мышь вынимается из подставки и используется по назначению;
- сканер сосудистого русла, совмещенный со считывателем контактной смарт-карты (PalmSecure);
- сканер сосудистого русла, совмещенный со считывателем бесконтактных смарт-карт (ОКБ САПР, на базе сканера PalmSecure).

Сканер сосудистого русла, совмещенный с манипулятором мышь

Сканер сосудистого русла, совмещенный со считывателем контактной смарт-карты

Сканер сосудистого русла, совмещенный со считывателем бесконтактных смарт-карт

Программы профессиональной переподготовки и повышения квалификации специалистов в области технической защиты информации (ТЗИ), согласованные с ФСТЭК России

№	Наименование программы	Категория слушателей	Документ об окончании обучения	Продолжительность (ак. ч.)
Программы профессиональной переподготовки				
1	**ТЗИ ограниченного доступа, не содержащей сведения, составляющие государственную тайну**	Специалисты (включая государственных гражданских служащих) в области технической защиты конфиденциальной информации	Диплом о профессиональной переподготовке	706
2	**Информационная безопасность. Техническая защита конфиденциальной информации**	Специалисты, работающие в области ТЗИ	Диплом о профессиональной переподготовке	470
Программы повышения квалификации				
3	**ТЗИ. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну**	Руководители и сотрудники (включая государственных гражданских служащих), работающие в области ТЗИ, в части организации защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну	Удостоверение о повышении квалификации	216

№	Наименование программы	Категория слушателей	Документ об окончании обучения	Продолжи-тельность (ак. ч.)
4	**ТЗИ. Способы и средства защиты информации от несанкционированного доступа**	Специалисты (включая государственных гражданских служащих), работающие в области ТЗИ в части выбора и применения способов и средств защиты информации от несанкционированного доступа	Удостоверение о повышении квалификации	108
5	**Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры**	Специалисты (включая государственных гражданских служащих) субъектов критической информационной инфраструктуры (КИИ), ответственных за обеспечение безопасности значимых объектов КИИ	Удостоверение о повышении квалификации	216

Программы профессиональной переподготовки и повышения квалификации специалистов

№	Наименование программы	Категория слушателей	Документ об окончании обучения	Продолжи-тельность (ак. ч.)
Программа профессиональной переподготовки				
1	**Технологии и средства обеспечения компьютерной безопасности**	Системные администраторы, Специалисты по информационным технологиям, Специалисты по информационной безопасности, Специалисты технической поддержки, Офицеры	Диплом о профес-	540

№	Наименование программы	Категория слушателей	Документ об окончании обучения	Продолжи-тельность (ак. ч.)
	(программа согласована с ФСБ России)	информационной безопасности, Руководители ИТ- и ИБ-подразделений	сиональной переподготовке	
Программы повышения квалификации				
2	**Технологии и средства защиты компьютерных систем**	Системные администраторы, Специалисты по информационным технологиям, Специалисты по информационной безопасности, Специалисты технической поддержки, Офицеры информационной безопасности, Руководители ИТ- и ИБ-подразделений	Удостоверение о повышении квалификации	102
3	**Защита информации в ИСПДн, ГИС и значимых объектах КИИ**	Лица, имеющие высшее образование по одному из направлений УГНП 10.00.00 «Информационная безопасность» или высшее образование и прошедшие профессиональную переподготовку в области информационной безопасности или технической защиты информации, и желающие повысить свою квалификацию в данной области.	Удостоверение о повышении квалификации	72

Специализированные программы

№	Наименование программы	Назначение программы	Документ, выдаваемый по окончанию обучения	Продолжи-тельность (ак. ч.)
1	**Управление рисками информационной безопасности** • Нормативное обеспечение управления рисками ИБ • Основные этапы управления рисками ИБ	Курс предназначен и будет полезен для директоров служб автоматизации (CIO), служб безопасности (CISO), а также для исполнительных директоров (CEO) в постановке и решении задач анализа информационных рисков и управления ими, оценки непрерывности бизнеса, оценки экономической эффективности корпоративных систем защиты информации и др.	Сертификат об окончании курса /Сертификат с оценкой	68
2	**Системы охранного телевидения** • Получение информативного телевизионного сигнала в широком диапазоне изменения внешних условий и разнообразии оперативных задач • Комплекс сбора и отображения видеоинформации	Курс предназначен для технических специалистов службы безопасности предприятия и будет полезен для аналитического отдела службы безопасности	Сертификат об окончании курса /Сертификат с оценкой	68

3	**Системы физической защиты** • Основы построения комплекса систем физической защиты • Комплекс инженерно-технических систем физической защиты	Курс предназначен для директоров служб безопасности (CISO) для оценки рисков физической безопасности, выбора оптимального способа противодействия реальным угрозам в меняющейся обстановке, оценки эффективности применяемой системы физической защиты и оптимизации инвестиций в составные части системы	Сертификат об окончании курса /Сертификат с оценкой	51
4	**Стандарты Банка России в области информационной безопасности**	Курс предназначен для сотрудников отдела информационной безопасности в банковской сфере, руководителей отдела ИБ в банковской сфере	Сертификат об окончании курса /Сертификат с оценкой	16/32
5	**Криптографические методы защиты информации**	Курс предназначен для специалистов в области разработки, модернизации, производства, монтажа и установки шифровальных (криптографических) средств. Курс будет полезен специалистам, разрабатывающим информационные и телекоммуникационные системы, защищенные с использованием шифровальных (криптографических) средств	Сертификат об окончании курса /Сертификат с оценкой	72

6	**Прикладная криптография**	Курс предназначен для лиц, работающих в сфере разработки, внедрения и эксплуатации программно-аппаратных средств защиты информации, разработки информационно-телекоммуникационных систем с применением средств криптографической защиты информации, специалистов в области цифровой экономики и блокчейн-технологий. Курс будет полезен для лиц, работающих в сфере распространения средств криптографической защиты информации, специалистов по управлению информационной безопасностью	Сертификат об окончании курса /Сертификат с оценкой	36/72/102
7	**Нормативные аспекты разработки и использования средств криптографической защиты информации**	Курс предназначен для специалистов, занимающихся разработкой, производством и эксплуатацией средств криптографической защиты информации. Курс полезен для специалистов, применяющих в рамках профессиональной деятельности средства криптографической защиты информации	Сертификат об окончании курса /Сертификат с оценкой	36/64/72
8	**Защита информации в банковских системах**	Курс предназначен для специалистов отделов информационной безопасности банков и финансовых организаций, осуществляющих переводы денежных средств. Курс полезен сотрудникам организаций, выполняющих требования 382-П и СТО БР ИББС	Сертификат об окончании курса /Сертификат с оценкой	24

9	**Анализ данных и машинное обучение с приложениями в кибербезопасности**	Курс предназначен для лиц, работающих в сфере разработки и применения интеллектуальных средств и систем обеспечения информационной безопасности: систем обнаружения и предотвращения вторжений, SIEM-систем, поведенческой биометрии, компьютерной форензики и др. Курс будет полезен для специалистов по обеспечению информационной безопасности в сфере цифровой экономики, администраторам информационной безопасности организаций	Сертификат об окончании курса /Сертификат с оценкой	36/72
10	**Организационное и правовое обеспечение информационной безопасности**	Курс предназначен для специалистов отделов информационной безопасности широкого спектра организаций с целью обеспечения соответствия требованиям законодательства РФ в области защиты и обработки персональных данных. Курс полезен слушателям, занимающимся комплексным обеспечением информационной безопасности на предприятии, организацией и ведением конфиденциального документооборота	Сертификат об окончании курса /Сертификат с оценкой	40

Авторские программы

№	Наименование программы	Категория слушателей	Документ, выдаваемый по окончанию обучения	Продолжи-тельность (ак. ч.)
1	**Применение и администрирование продуктов ОКБ САПР**	Сотрудники отдела информационной безопасности, руководители отдела ИБ, администраторы СЗИ	Сертификат об окончании курса /Сертификат с оценкой	49
2	**Применение и администрирование ПАК СЗИ от НСД семейства «Аккорд»**	Сотрудники отдела информационной безопасности, руководители отдела ИБ, администраторы СЗИ	Сертификат об окончании курса /Сертификат с оценкой	34,5
3	**Защита виртуальных инфраструктур на основе ПАК «Аккорд-В.» и «Сегмент-В.»**	Сотрудники отдела информационной безопасности, администраторы СЗИ	Сертификат об окончании курса /Сертификат с оценкой	18
4	**Технологии защищенного применения служебных USB-накопителей**	Сотрудники отдела информационной безопасности, руководители отдела ИБ, администраторы СЗИ	Сертификат об окончании курса /Сертификат с оценкой	8,5
5	**Технология доверенного сеанса связи и средство обеспечения доверенного сеанса связи "МАРШ!"**	Сотрудники отдела информационной безопасности, руководители отдела ИБ, администраторы СЗИ	Сертификат об окончании курса /Сертификат с оценкой	8

6	**Применение и администрирование защищенных микрокомпьютеров МКТ**	Сотрудники отдела информационной безопасности, руководители отдела ИБ, администраторы СЗИ	Сертификат об окончании курса /Сертификат с оценкой	68

Руководитель Обучающего центра ОКБ САПР Татьяна Михайловна Каннер ответит на все вопросы по организации обучения по почте tatianash@okbsapr.ru или по телефону +7 (926)235-14-67.

СПЕЦИАЛИЗИРОВАННЫЙ КОМПЬЮТЕР С АППАРАТНОЙ ЗАЩИТОЙ ДАННЫХ M-TRUST: ПЛАТФОРМА ДЛЯ ЗАЩИЩЕННЫХ РЕШЕНИЙ

Выполнение требований 187-ФЗ и связанных с ним подзаконных актов сопряжено с очень большим количеством организационных мероприятий, которые необходимо провести в кратчайшие сроки. На этом фоне необходимые технические меры не кажутся проблемой, тем более что принципиально задачи технической защиты информации и способы их решения профессионалам хорошо понятны. Однако при переходе к планированию выясняется, что с реализацией этих способов на практике все пока не так благополучно, как в теории.

Это связано с тем, что объекты защиты информации всех типов (технические средства, данные, информационные технологии, каналы передачи данных), в КИИ крайне разнообразны, намного разнообразнее, чем в среднем в защищенных корпоративных или государственных информационных системах (см. табл. 1).

Таблица 1. Особенности объектов защиты информации в КИИ

Объекты защиты информации	«обычные» защищенные ИС	КИИ
Технические средства	Сервера, ПК, терминалы	То же, плюс управляющие элементы КИИ, разнообразные

		датчики и контроллеры
Данные	Файлы и данные	То же, плюс сигналы управления, данные измерений и контроля
Каналы	Ethernet	То же, плюс WiFi, BlueTooth, LTE и др.
Информационные технологии	Прикладное ПО и общесистемное ПО	То же, плюс ПО управления технологическими процессами

Что особенно важно – все это разнообразие практически не может быть унифицировано, а значит,

мероприятия по защите КИИ должны повлечь за собой применение столь же разношерстных средств защиты информации, которые необходимо спроектировать, внедрить и сопровождать. Все это грозит весьма ощутимыми расходами.

Особенно выпукло картина выглядит на примере защиты сетевого взаимодействия объектов КИИ: защищено должно быть все, а не только информационный уровень системы. Обменивающиеся по сети разнообразными данными и сигналами технические средства объектов КИИ не только сами по себе разнообразны, но и располагаться могут весьма нетривиальным для обычных информационных систем образом – не только на стационарных, но и на мобильных и даже подвижных объектах[1].

При этом *на всех* местах выработки должны защищаться *все* сигналы и *все* каналы передачи данных.

В подавляющем большинстве КИИ непременной частью системы защиты сетевого взаимодействия являются средства криптографической защиты

[1] Хотя необходимо признать, что и стационарные объекты могут ощутимо различаться – от центрального офиса до станции общественного транспорта или, скажем, маяка, но все же размещение мобильных (банкомат, инфокиоск), а особенно – подвижных объектов (поезд, автомобиль инкассации, скорая помощь, корабль) отличается еще большей непредсказуемостью.

информации (СКЗИ), поскольку, как уже упоминалось, некоторые объекты КИИ взаимодействуют по незащищенным сетям общего доступа, причем с использованием стандартных цифровых каналов типа WiFi, BlueTooth и LTE. Изменение порядка взаимодействия с построением выделенных защищенных каналов не всегда возможно в принципе, а когда и возможно – то влечет за собой весьма продолжительные и дорогостоящие работы, несопоставимые с внедрением СКЗИ[2]. Со стороны СКЗИ же, в свою очередь, предъявляются требования к среде функционирования криптографии (СФК), условиям хранения и применения ключей и т. п.

Отсюда недвусмысленно вытекает набор свойств, которыми должна характеризоваться платформа средства защиты сетевого взаимодействия между объектами КИИ:

1) возможность создавать и поддерживать доверенную вычислительную среду,

2) возможность работы с неизвлекаемым ключом в автоматическом режиме,

3) возможность установки различных СКЗИ при соблюдении условий сертификации на высокие классы,

4) возможность работы с различными каналами связи по различным протоколам, при необходимости – параллельно,

[2] Откровенно говоря, даже не смешно представить себе такую постановку задачи для стоящего «в чистом поле» банкомата.

5) возможность коммутации с различным оборудованием объекта КИИ без модификации последнего.

Отдельно необходимо остановиться на том, что все эти характеристики касаются именно аппаратной платформы, а не программной реализации на ней конкретного решения.

Не оставаясь на уровне аксиоматики (приоритет аппаратной реализации защитных функций давно не нуждается в доказательствах), приведем самые очевидные аргументы.

Фактически, в части защиты сетевого взаимодействия все специфичное в требованиях к КИИ сводится к тому, что

> при взаимодействии с использованием сетей общего доступа *каждый узел* должен быть защищен СКЗИ *высокого класса*.

Все остальное – следствия из этого обстоятельства.

Детали сертификационных требований приведены в справочном разделе в конце этой брошюры.

Некоторые следствия, вытекающие из необходимости защиты всех узлов сети рассмотрим на примере защиты банкоматов.

Для оборудования каждого узла СКЗИ, сертифицированным на высокий класс, неприемлемо

использовать установленный на технические средства программный VPN. Даже в случае, если для него создана и поддерживается СФК, это недопустимо потому, что при обслуживании в ПО этого компьютера могут быть внесены изменения, нарушающие СФК, а проведение в каждом случае соответствующих проверок – просто невозможно организационно. Более того, в случае с рядом специфических объектов КИИ вообще возможна ситуация, что непредсказуемые изменения – например, замена компьютера на свой, улучшенный – будут произведены, например, при работах вообще не с компьютером, а с какими-то другими техническими средствами объекта – например, с диспенсером банкомата: объекты КИИ зачастую обслуживаются большим количеством технического персонала, среди которого может скрываться злоумышленник.

Ситуация выглядит несколько лучше при использовании аппаратного шлюза, однако, использование импортных устройств неприемлемо по причине их несоответствия требованиям регуляторов, а отечественные сертифицированные устройства в этом качестве, как правило, не используются. Причины на это, в общем, объективные – цена и габариты.



Не то что бы их нельзя было установить в каждый банкомат, электричку, машину инкассации, скорую помощь и инфокиоск, но они дороги, избыточны по своим характеристикам, очень велики по размеру и зачастую подвержены множеству уже хорошо разработанных и постоянно появляющихся новых атак.

Еще одно требование регулятора к СКЗИ высокого класса – неизвлекамый ключ. Казалось бы, эта тема должна быть раскрыта в современных СКЗИ в полной мере, однако и здесь есть важные для применения в КИИ особенности.

«Неизвлекаемость» – свойство, описывающее связь ключа с некоторым его физическим хранилищем, то есть говоря о том, что ключ неизвлекаем, необходимо уточнять, *откуда*. Неизвлекаемые ключи как правило неизвлекаемы из токена, который, как правило – USB-устройство, смарт-карта или «таблетка» Touch Memory. Читая документы на СКЗИ высоких классов сертификации для защиты канала, мы видим, что «требование неизвлекаемости ключа выполняется применением токена…». Это добросовестное выполнение требования, однако, токен с неизвлекаемым ключом – это инструмент решения совсем другой задачи, существенно отличающейся от защиты сетевого взаимодействия объектов КИИ. Токен предназначен для того, чтобы ключ *пользователя* был *отчуждаем* от СВТ, на котором пользователь

осуществляет те или иные операции с ключом. В описываемом же случае отчуждаемость не только избыточна, но и вредна: с одной стороны, она делает возможными сценарии атак с подменой или иными вариантами компрометации ключа за счет отчуждаемости его носителя, а с другой, подключенное к порту USB-устройство резко снижает надежность решения – при вибрации, ударах, нагревании и прочих особенностях условий, в которых работают технические средства на объектах КИИ.

Модуль работы с неизвлекаемом ключом должен быть реализован как часть резидентного компонента безопасности, размещенного непосредственно на плате компьютера, а не как отчуждаемый персональный носитель ключа.

Задачи коммутации и использования широкого спектра каналов и протоколов связаны уже не с требованиями регуляторов, а с техническими особенностями объектов КИИ. необходимо поддержать множество различных интерфейсов, то есть тоже требуют аппаратных решений.

Всем этим требованиям отвечает специализированный компьютер с аппаратной защитой данных m-TrusT.

Его особенностями являются:

- Новая гарвардская архитектура, обеспечивающая вирусный иммунитет

- аппаратная поддержка реализации доверенной загрузки
- функциональная замкнутость среды
- аппаратное обеспечение целостности
- аппаратное резидентное решение по неизвлекаемости ключа
- аппаратный ДСЧ.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 191690

СПЕЦИАЛИЗИРОВАННЫЙ КОМПЬЮТЕР С АППАРАТНОЙ ЗАЩИТОЙ ДАННЫХ

Патентообладатели: *Закрытое акционерное общество "Особое Конструкторское Бюро Систем Автоматизированного Проектирования" (RU), Пярин Виктор Анатольевич (RU), Общество с ограниченной ответственностью "Сангар" (RU)*

Авторы: *Батраков Антон Юрьевич (RU), Коняевский Валерий Аркадьевич (RU), Счастный Дмитрий Юрьевич (RU), Пярин Виктор Анатольевич (RU)*

Заявка № 2019115393
Приоритет полезной модели **20 мая 2019 г.**
Дата государственной регистрации в Государственном реестре полезных моделей Российской Федерации **15 августа 2019 г.**
Срок действия исключительного права на полезную модель истекает **20 мая 2029 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Однако, кроме архитектурного решения, необходимо определить также форм-фактор и эксплуатационные требования, с соблюдением которых нужно изготовить компьютер.

Если во все уже функционирующие объекты КИИ внедрить средства защиты, которые будут обеспечивать:

1) криптографическую защиту ***всей*** передаваемой информации;

2) информационное взаимодействие ***всех*** объектов КИИ;

3) возможность использования ***разнообразных*** цифровых каналов (WiFi, BlueTooth, и др.);

4) информационное взаимодействие с ***разнообразной*** каналообразующей аппаратурой (RS232, RS435 и др.)

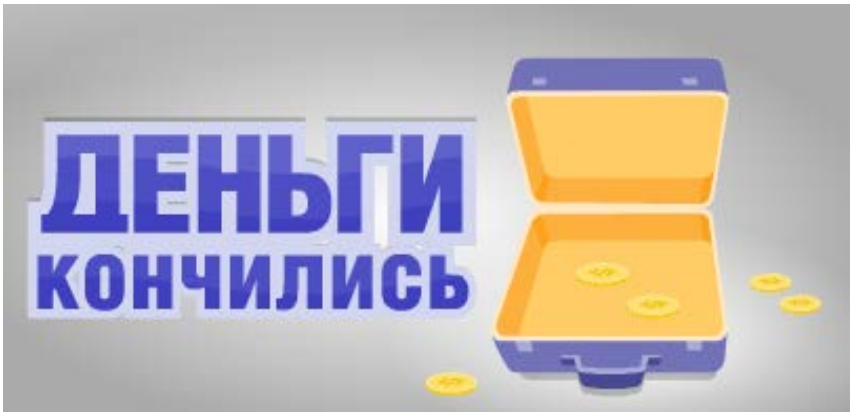
и все это – для ***всех*** типов технических средств, то при традиционном подходе это приведет к:

1) серьезной ***переработке проектных решений***;

2) ***модернизации*** исправного и еще не выработавшего свой ресурс оборудования;

3) ***восстановлению системы после сбоев***, вызванных модернизацией, которая может привести к частичному или полному нарушению функционирования системы.

Защита выльется в серьезные финансовые затраты.



Но вариантов исполнения требований 187-ФЗ несколько. Можно:

1) провести модернизацию объектов КИИ;

2) для каждого объекта КИИ разработать, изготовить и сертифицировать собственное множество аппаратных СКЗИ;

3) создать специальную аппаратуру, обладающую всеми необходимыми свойствами, и особенностью которой будет простейшая модернизация к любым объектам и каналам, не требующая проведения повторной сертификации.

Очевидно, что:

- первый вариант очень дорогой и длительный,

- второй – дорогой и очень длительный,

Причем в обоих случаях приведение системы в соответствие с требованиями закона и подзаконных актов тем дороже, чем выше разнообразие технических средств в системе.

- третий – полностью приемлем, если цена решения будет доступной.

Адаптация СЗИ к техническим средствам объектов КИИ позволит сохранить инвестиции в КИИ.

Однако адаптация СЗИ, а особенно – СКЗИ – это повторная сертификация. Замкнутый круг?

Нет, инженерная задача.

Решается задача путем декомпозиции: разделения СЗИ на то, что должно быть неизменным, чтобы не требовалось повторной сертификации, и то, что может меняться для того, чтобы интегрироваться с очередным техническим средством на очередном объекте КИИ.

Для разработки решения по лучшему варианту нужно выделить аппаратное ядро, а встраивание выполнять за счет создания несложных интерфейсных плат, обеспечивающих транспорт и необходимый форм-фактор, но не связанных с выполнением криптографических функций.

Ядро проектируется как универсальное, множество интерфейсных плат может быть огромно, форм-факторы разнообразны и зависят только от особенностей объектов КИИ.

Такое решение создано – это защищенная интеграционная платформа МК-И.

МК-И – это микрокомпьютер Новой гарвардской архитектуры m-TrusT и интерфейсная плата для его коммутации с сетевой инфраструктурой, которая может включать в себя самые разные типы оборудования. Поэтому интерфейсные платы делаются различными, а сам микрокомпьютер m-TrusT – универсальный, его форм-фактор не зависит от предполагаемого места установки.

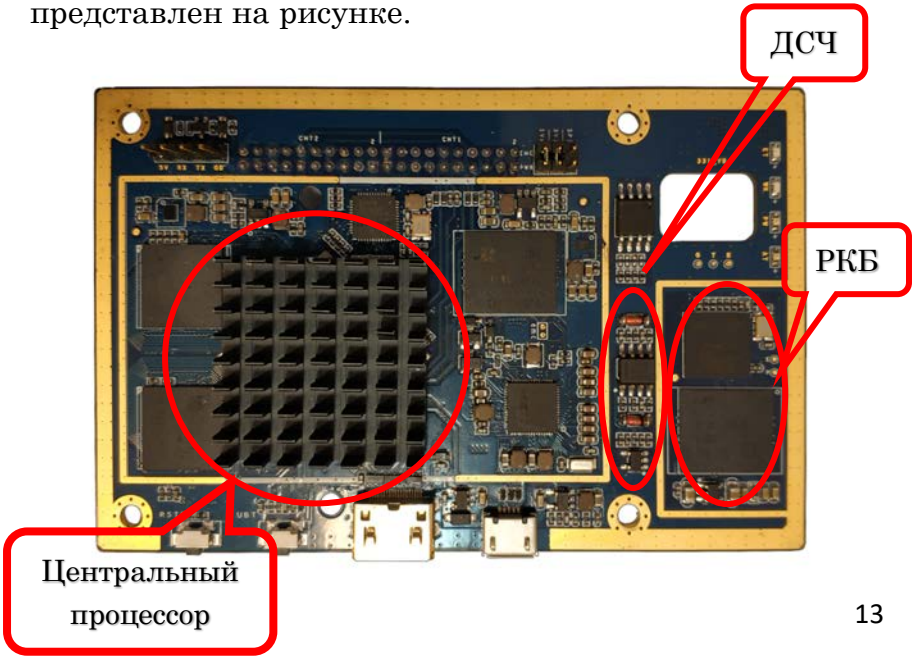
Важно это потому, что изменения интерфейсной части не влияют на вычислительную часть компьютера, а это снимает основные сложности, вызываемые адаптацией серийного продукта – возможное внесение новых ошибок или дефектов, необходимость повторных проверок или сертификации и т. п. Ядро универсально, а интерфейсные платы обеспечивают только транспорт.

Каждый микрокомпьютер «m-TrusT» является точкой сбора информационных и/или управляющих сигналов от объектов КИИ, их шифрования для передачи по каналам связи, а также приема зашифрованных сигналов из каналов связи и их расшифровкой.

Типовые характеристики микрокомпьютеров:

- Габаритные размеры: 65 х 80 мм;
- Процессор: Quad-core ARM Cortex-A17, up to 1.8 GHz;
- ОЗУ: 2 Гб DDR3;
- ПЗУ: 16 Гб NAND-flash;
- microUSB;
- microHDMI.

Общий вид микрокомпьютера m-TrusT представлен на рисунке.



Микрокомпьютер не подключается напрямую ни к чему, кроме собственной интерфейсной платы, поэтому его состав не сложен и постоянен. Интерфейсная плата же нужна как раз для того, чтобы корректно подключиться к тому или иному конкретному ПКО и каналообразующей аппаратуре различных типов.

Наличие собственной ОС и вычислительных ресурсов позволяет обеспечить достаточную для защиты сетевого взаимодействия производительность[3] и высокий уровень защищенности. Особенностями m-TrusT является наличие датчика случайных чисел и размещение ПО в памяти с физически устанавливаемым доступом read only (только чтение), что исключает вредоносное воздействие на ПО и обеспечивает неизменность среды функционирования средств криптографической защиты информации. Ресурсы m-TrusT позволяют обеспечить СФК, позволяющую сертифицировать вариант исполнения СКЗИ на m-TrusT на класс КС3. Помимо Новой гарвардской архитектуры защищенность платформы обеспечивается РКБ и СДЗ, сертифицированным ФСТЭК России.

Встроенное СКЗИ может быть любым сертифицированным[4].

[3] Возможна защищенная передача видеосигнала с камер без ощутимого снижения качества изображения.

[4] Например, в решении «fin-TrusT» для защиты сетевого взаимодействия в финансовой организации встроенное СКЗИ – DCrypt от компании ТСС.

Итак, коммутировать микрокомпьютер m-TrusT в «разрыв» между ПКО различного назначения и каналом связи позволяет интерфейсная плата. Как уже упоминалось – разнообразие оборудования, взаимодействующего по сети (ПК, скорая помощь, банкомат, электричка, информационный киоск, машина инкассации, терминал оплаты etc), является ключевой характеристикой инфраструктуры, поэтому интерфейсные платы должны быть ***разными***, чтобы коммутировать ***одно и то же*** СЗИ (то есть не *совместимые*, не *похожие*, а именно *одинаковые* СЗИ) с разными ПКО. Например, она может быть такой, как на рисунке:

- Габаритные размеры: 90 х 105 мм;
- Соединитель типа Розетка 87758-2016 MOLEX;
- Разъем USB Type A;
- Разъем Ethernet;
- Разъем питания от источника постоянного напряжения 5 вольт.

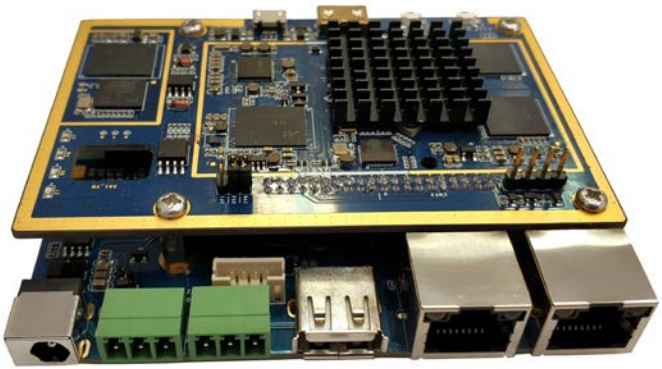
Интерфейсная плата №2

- Габаритные размеры 90 х 110 мм;
- Соединитель типа Розетка 87758-2016 MOLEX;
- USB-хаб;
- Разъем USB Type A;
- 2 разъема Ethernet ;
- Разъем RS-232, подключенный через преобразователь USB-RS-232;

• Разъем RS-485, подключенный через преобразователь USB-RS-485;

• Разъем для micro-SD карты;

• Разъем питания от источника постоянного напряжения 5 вольт.



На следующем рисунке показан другой вариант интерфейсной платы с меньшим количеством интерфейсных разъемов:

• Габаритные размеры: 90 x 105 мм

• Соединитель типа Розетка 87758-2016 MOLEX

• Разъем USB Type A

• Разъем Ethernet

• Разъем питания от источника постоянного напряжения 5 вольт.

Возможна разработка интерфейсных плат для других типов разъемов. С учетом уже имеющегося опыта внедрения на транспорте и кредитно-финансовой сфере, мы уверенно говорим о том, что эта

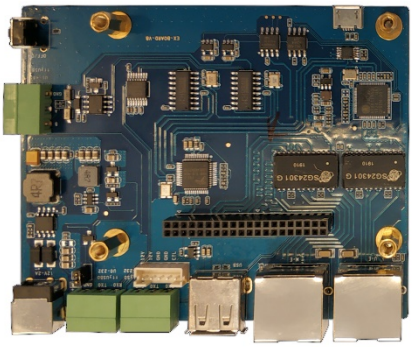
задача решается с положительным результатом в разумные сроки.

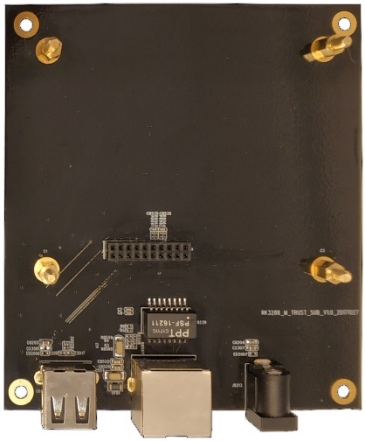
Для некоторых объектов, как показала практика, удобным может быть исполнение в едином корпусе, например, если частого переоборудования не требуется, а техническое средство функционирует вне помещения, где внешние условия могут быть разнообразными и не всегда благоприятными. В этом случае корпус снижает возможное воздействие внешних условий.

Разумеется, за счет описанных особенностей МК-И, построенное на нем решение может поддержать любой из вариантов связи объектов, или даже все их одновременно, причем с дублированием каждого канала (несколько каналов Ethernet, несколько sim-карт для мобильного Интернета и т. д.), с тем чтобы во время работы использовать тот, что доступен в данный момент и в данном месте.

Такое средство защиты универсально – на все технические средства всех объектов системы

внедряется одно и то же СЗИ без внесения каких-либо изменений в само защищаемое оборудование. Эта универсальность обеспечивается интерфейсными платами.





Еще раз подчеркнем, что такая платформа *уже создана*, запатентована[5], решения, построенные на ней сертифицированы, внедряются и применяются в реальных функционирующих КИИ. Ее преимущества – кроме сертифицированных ФСТЭК и ФСБ России встроенных средств защиты и «вирусного иммунитета» – достаточная производительность при низкой цене.

[5] Описание полезной модели к патенту Вы можете увидеть в конце этой брошюры.

ОСНОВНЫЕ ОСОБЕННОСТИ, ОБЕСПЕЧИВАЮЩИЕ ЗАЩИЩЕННОСТЬ РЕШЕНИЯ

Самое главное свойство платформы – полная доверенная загрузка, то есть доверенная загрузка не только ОС, но и начальная загрузка устройства полностью контролируемая, с пошаговым обеспечением целостности, позволяющим поддерживать среда функционирования криптографии.

Процессор устройства сконфигурирован таким образом, чтобы старт загрузки всегда производился из памяти, аппаратно защищенной от перезаписи (физически переведенной в режим read only). Из этой памяти стартует загрузчик, который проверяет целостность модуля, который, стартовав, производит настройку СДЗ. Последний в свою очередь контролирует старт ОС. Эта схема обеспечивает пошаговый контроль загрузки, который позволяет сделать старт микрокомпьютера доверенным на всем его протяжении.

Доверенная загрузка поддерживается программным комплексом Аккорд-МКТ, сертифицированным ФСТЭК.

Функциональная замкнутость среды поддерживается комплексом Аккорд-Х, сертифицированным ФСТЭК.

СИСТЕМА СЕРТИФИ
СРЕДСТВ ЗАЩИТЫ ИНФ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНО
№ РОСС RU.0001.0

СЕРТИФИКАТ СООТВЕ
№ 3936

Выдан 10 мая 2018 г.
Действителен до 10 мая 2021 г.

Настоящий сертификат удостоверяет, что модуль до
МКТ», разработанный и производимый ЗАО «ОКБ САПР»
условиями ТУ 501410-071-37222406-2016, является програм
загрузки, соответствует требованиям документов «Требов
загрузки» (ФСТЭК России, 2013) и «Профиль защиты средс
базовой системы ввода-вывода четвертого класса защиты. ИТ
2013) при выполнении указаний по эксплуатации,
37222406.501410.071 ФО.

Сертификат выдан на основании результатов с
проведенных испытательной лабораторией ООО «ЦБИ» (атте
№ СЗИ RU.0001.01БИ00.Б004) - техническое заключени
заключения от 04.04.2018 органа по сертификации ФАУ «Г
(аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.

Заявитель: ЗАО «ОКБ САПР» (ИНН 7725739137)
Адрес: 117525, г. Москва, ул. Автозаводская, д. 1
Телефон: (499) 235-6265

Контроль маркирования знаками соответствия с
и инспекционный контроль её соответствия требованиям доку
сертификате, осуществляется испытательной лабораторией ОО

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭ

Настоящий сертификат внесен в Государственный реестр сертификатов
10 мая 2018 г.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3079

Выдан 30 января 2014 г.
Действителен до 30 января 2017 г.
Срок действия продлен до 30 января 2020 г.

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X», разработанный и производимый ЗАО «ОКБ САПР» в соответствии с техническими условиями ТУ 4012-026-11443195-2008, функционирующий в средах операционных систем, указанных в формуляре 11443195.4012.026 ФО, является программно-техническим средством защиты информации от несанкционированного доступа, реализующим функции идентификации и аутентификации, управления доступом, очистки памяти, регистрации событий безопасности, контроля целостности, соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 2 уровню контроля, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 3 классу защищенности и технических условий при выполнении ограничений по применению, указанных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации», (аттестат аккредитации от 30.03.2006 № СЗИ RU.117.Б08.025) – техническое заключение от 13.12.2013, и экспертного заключения от 27.12.2013 органа по сертификации ЗАО «Лаборатория ППШ» (аттестат аккредитации от 29.09.2007 № СЗИ RU.054.A97.010) и результатов инспекционного контроля, проводимого испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001) - техническое заключение от 28.02.2017.

Заявитель: ЗАО «Особое Конструкторское Бюро Систем Автоматизированного Проектирования» (ИНН 7725739137)
Адрес: 115280, г. Москва, ул. Автозаводская, д.1
Телефон: (499) 235-6265

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов и технических условий, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
30 января 2014 г.

А также:

- физический датчик случайных чисел – двухплечевое решение с использованием диодов 2Г103А9, по схеме «Дебют», имеет положительное заключение ФСБ;

- криптографическое API поддержки аппаратного неизвлекаемого ключа платформы m-TrusT имеет положительное заключение ФСБ;

- специализированный компьютер с аппаратной защитой данных m-TrusT сертифицирован ФСБ как платформа для СКЗИ DCrypt на класс КС3.

Как любой универсальный защищенный компьютер, m-TrusT может использоваться для реализации всех технических мер обеспечения безопасности значимых объектов КИИ, включая ИАФ, УПД, ОПС, ЗНИ, АУД, АВЗ, СОВ, ОЦЛ, ОДТ, ОПО. Наиболее же эффективно использовать m-TrusT для обеспечения группы мер ЗИС.

При использовании m-TrusT в составе ИС важно соответствие требованиям регулятора его собственных свойств. Этому посвящена таблица 2. В таблице 3 же приведены те меры, которые обеспечиваются с помощью m-TrusT в системах КИИ.

Таблица 2. Соответствие m-TrusT техническим мерам Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие m-TrusT требованиям ФСТЭК	Примечание
I. Идентификация и аутентификация (ИАФ)			Меры ИАФ.0. ИАФ.3, ИАФ.4 являются организационными. Мера ИАФ.6 – необязательная.
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	
ИАФ.2	Идентификация и аутентификация устройств	+	

ИАФ.5	Идентификация и аутентификация внешних пользователей	+	
ИАФ.7	Защита аутентификационной информации при передаче	+	
II. Управление доступом (УПД)			Меры УПД.0, УПД.4, УПД.5 являются организационными. Меры УПД.7, УПД.8, УПД.12 – необязательные.
УПД.1	Управление учетными записями пользователей	*	Не имеет пользователей т. к. обычно работает в автоматическом режиме
УПД.2	Реализация модели управления доступом	*	Управление доступом осуществляется ключевой системой
УПД.3	Доверенная загрузка	+	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	
УПД.9	Ограничение числа параллельных сеансов доступа	*	Ограничивается ключевой системой

УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	
УПД.13	Реализация защищенного удаленного доступа	+	Защита удаленного доступа обеспечивается СКЗИ
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	
III. Ограничение программной среды (ОПС)			Меры ОПС.0 и ОПС.2 являются организационными. Мера ОПС.3 – необязательная.
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+	

IV. Защита машинных носителей информации (ЗНИ)			Меры ЗНИ.0 - ЗНИ.2 являются организационными. Меры ЗНИ.3 и ЗНИ.4 – необязательные.
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. В системе обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.7	Контроль подключения съемных машинных носителей информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	-	

V. Аудит безопасности (АУД)			Меры АУД.0 – АУД.2, АУД.10 и АУД.11 являются организационными.
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	Обеспечивается собственной системой времени
АУД.4	Регистрация событий безопасности	+	
АУД.5	Контроль и анализ сетевого трафика	-	
АУД.6	Защита информации о событиях безопасности	+	
АУД.7	Мониторинг безопасности	+	
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	
АУД.9	Анализ действий отдельных пользователей	-	

VI. Антивирусная защита (АВЗ)			Меры АВЗ.0 и АВЗ.5 являются организационными.
АВЗ.1	Реализация антивирусной защиты	+	
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	-	Электронная почта и внешние сервисы не используются
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	-	
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	-	Не требуется
VII. Предотвращение вторжений (компьютерных атак) (СОВ)			Мера СОВ.0 является организационной.
СОВ.1	Обнаружение и предотвращение компьютерных атак	**	Обеспечивается внешними средствами СОВ

СОВ.2	Обновление базы решающих правил	**	Обеспечивается внешними средствами СОВ
VIII. Обеспечение целостности (ОЦЛ)			Мера ОЦЛ.0 является организационной. Меры ОЦЛ.2 и ЗНИ.6 – необязательные.
ОЦЛ.1	Контроль целостности программного обеспечения	+	
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	+	
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+	
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+	

IX. Обеспечение доступности (ОДТ)			Меры ОТД.0 – ОТД.2 являются организационными. Мера ОТД.7 – необязательная.
ОДТ.4	Резервное копирование информации	**	В соответствии с политикой информационной безопасности
ОДТ.5	Обеспечение возможности восстановления информации	**	В соответствии с политикой информационной безопасности
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	Обеспечивается архитектурой
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	-	

X. Защита технических средств и систем (ЗТС)			Меры ЗТС.0, ЗТС.2 – ЗТС.5 являются организационными. Меры ЗТС.1 и ЗТС.6 – необязательные.
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			Меры ЗИС.0 – ЗИС.5, ЗИС.8 являются организационными. Меры ЗИС.7, ЗИС.9 – ЗИС.12, ЗИС14, ЗИС.15, ЗИС.17, ЗИС.18, ЗИС.22 – ЗИС.26, ЗИС.28 – ЗИС.31, ЗИС.36, ЗИС.37 – необязательные.
ЗИС.6	Управление сетевыми потоками	+	Обеспечивается ключевой системой
ЗИС.13	Защита неизменяемых данных	+	
ЗИС.16	Защита от спама	+	
ЗИС.19	Защита информации при ее передаче по каналам связи	+	
ЗИС.20	Обеспечение доверенных канала, маршрута	+	
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	

ЗИС.27	Обеспечение подлинности сетевых соединений	+	
ЗИС.32	Защита беспроводных соединений	+	
ЗИС.33	Исключение доступа через общие ресурсы	+	
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	
ЗИС.35	Управление сетевыми соединениями	+	
ЗИС.38	Защита информации при использовании мобильных устройств	+	
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	-	

XII. Реагирование на компьютерные инциденты (ИНЦ)			Все меры этой группы – организационные.
XIII. Управление конфигурацией (УКФ)			Все меры этой группы – организационные.
XIV. Управление обновлениями программного обеспечения (ОПО)			Меры ОПО.0, ОПО.1 и ОПО.3 являются организационными.
ОПО.2	Контроль целостности обновлений программного обеспечения	+	
ОПО.4	Установка обновлений программного обеспечения	+	
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)			Все меры этой группы – организационные.
XVI. Обеспечение действий в нештатных ситуациях (ДНС)			Все меры этой группы – организационные.
XVII. Информирование и обучение персонала (ИПО)			Все меры этой группы – организационные.

* - при использовании в ИС без СКЗИ мера осуществляется установкой СПО СЗИ

** - при использовании в ИС при установке СПО СЗИ

Таблица 3. Применение m-TrusT для защиты значимых объектов КИИ

Обозначение и номер меры	Меры обеспечения безопасности
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.27	Обеспечение подлинности сетевых соединений
ЗИС.32	Защита беспроводных соединений
ЗИС.33	Исключение доступа через общие ресурсы
ЗИС.35	Управление сетевыми соединениями

При этом m-TrusT обеспечивает существенные преимущества, в том числе:

1. Работа в автоматическом режиме, что существенно снижает нагрузку на организационно-технические меры при эксплуатации СКЗИ
2. Изменение форм-фактора без повторной сертификации изделия, что значительно сокращает сроки работ по защите КИИ
3. Обеспечивается работа с любыми каналами связи, используемыми в КИИ
4. Обеспечивается защита КИИ без глубокой переработки ее структуры, что сильно сокращает затраты на проведение мероприятий.

ОСОБЫЕ ВАРИАНТЫ

Немало уже написано о том, что встраиваемость в разнообразные технические средства различных объектов разных КИИ обеспечивается интерфейсными платами. Разработка интерфейсной платы под конкретное оборудование не занимает много времени и не влияет на защитные свойства и функции платформы.

В то же время не на всех объектах КИИ это требуется – некоторые из них могут быть офисными или серверными объектами, в таких случаях гораздо уместнее и соответствующее исполнение платформы для СЗИ. Для таких объектов платформа изготавливается для размещения в стойку или на столе.

Именно поэтому мы утверждаем, что m-TrusT – универсальное решение. Использование в качестве платформы для средства защиты сетевого

взаимодействия в КИИ специализированного компьютера с аппаратной защитой данных m-TrusT позволяет учитывать все особенности оборудования объектов КИИ и без затрат на перепроектирование и восстановление от сопутствующих сбоев, в кратчайшие сроки выполнить требования 187-ФЗ, сохранив при этом существующую структуру и логику функционирования.

Адаптация СЗИ к системе и к ее конкретному объекту – это не задача эксплуатирующей организации, это задача производителя СЗИ. И она решена.

ОСОБЫЕ УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ

Для систем класса АСУТП и КИИ особое значение имеют климатические условия. Специализированные компьютеры m-TrusT могут изготавливаться для категорий C (castom), I (industrial), M (military). Стандартное решение – I.

ПРОТОКОЛ
климатических испытаний модуля m-TrusT на базе RK3399

Место испытаний: НИИАС, г. Москва, Нижегородская ул., 27, стр. 1
Стенд для испытаний: Климатическая испытательная камера Tabai MC-81. Оборудование имеет поверку до 12.2019 г.
Оборудование для испытаний:

1. МПУЛ-И с установленным m-TrusT RK3399 (далее МПУЛ)
2. Док-станция с установленным m-TrusT RK3399 (далее док-станция)

Техническими условиями на МПУЛ-И установлены температурные границы от -20° до +50°.

Методика испытаний:

1. Охлаждение выключенного оборудования до -30°. Включение, проверка работоспособности.
2. Охлаждение выключенного оборудования до -40°. Включение, проверка работоспособности.
3. Нагрев включенного оборудования до +50°. Выключение, включение, проверка работоспособности.
4. Нагрев включенного оборудования до +60°. Выключение, включение, проверка работоспособности.

Температура считывается программно с двух датчиков на m-TrusT, температура среды определяется по датчику климатической камеры.

Результаты испытаний:

1. Охлаждение, удерживание температуры -30° в течении 1 часа, включение оборудования, температура на датчиках после включения МПУЛ -18°, док-станция -27°. После включения оборудование работало в штатном режиме.

2. Охлаждение, удерживание температуры -40° в течении 30 минут, включение оборудования, температура на датчиках после включения МПУЛ -30°, док-станция -38°. После включения оборудование работало в штатном режиме.

3. Нагрев оборудования до +50° и удерживание в течении 1 часа. Выключение-включение оборудования, температура МПУЛ +75°, док-станция +54°. После включения оборудование работало в штатном режиме.

4. Загрузка процессора m-TrusT на 100% в течении 5 минут при температуре +50°. Выключение-включение оборудования, температура МПУЛ 85°, док-станция 66°. После включения оборудование работало в штатном режиме.

5. Нагрев оборудования до +60 и удерживание в течении 1 часа. Выключение-включение оборудования, температура МПУЛ +92°, док-станция +66°. После включения оборудование работало в штатном режиме.

6. Загрузка процессора m-TrusT на 100% в течении 5 минут при температуре +60°. Выключение-включение оборудования, температура МПУЛ +100°, док-станция 76°. После включения оборудование работало в штатном режиме.

РЕШЕНИЯ НА БАЗЕ M-TRUST

Архитектура платформы с интерфейсной платой обуславливает возможность построения на базе специализированного компьютера с аппаратной защитой данных m-TrusT широкого спектра инфраструктурных решений.

Безопасный город

Нас окружают камеры, данные с которых оказывают непосредственное влияние на принятие множества критически важных или просто значимых для конкретных граждан решений. Изображение с этих камер передается по каналам передачи данных общего пользования, вмешательство в этот процесс «человека посередине» не представляет для злоумышленника сложности.

Такая атака дает злоумышленнику возможность подменять данные на те, что позволят ему решить какие-то свои задачи, либо, что не менее опасно, особенно в условиях движения к биометрической идентификации, – накапливать данные о гражданах в целях дальнейшего использования в собственных целях.

Встраивание в камеры СКЗИ на платформе m-TrusT сделает процесс сбора данных с камер защищенным с максимально возможным сохранением инвестиций. Стоимость оборудования камер СКЗИ

будет ощутимо ниже замены всех камер на такие, в которые по умолчанию встроены средства шифрования аналогичного класса защиты. «Безопасный» город становится безопасным.

Умный дом

Умный дом сейчас едва ли не в большей степени ассоциируется с опасностью, чем с прогрессом. Приборы, взаимодействующие по сети в лучшем случае разовьют искусственный интеллект и взбунтуются (это оптимистический сценарий, потому что случится это очень нескоро), а в худшем – попадут под управление не собственного хозяина, а его недоброжелателя. Можно рисовать много сценариев развития этой ситуации – как смешных, так и страшных. Оставив эту задачу сценаристам, можно решить проблему радикально – защитить взаимодействие вещей, поскольку от него зависят люди.

При этом сценарии m-TrusT со специализированной платой расширения становится концентратором потоков информационного взаимодействия в системах IoT (так называемого «Интернета вещей»). Преступник больше не сможет отключить ваш холодильник и включить кипяток в душе. Умный дом становится безопасным.

Надежный банк

Криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации fin-TrusT уже упоминался выше. С помощью криптошлюзов fin-TrusT защищаются коммуникации между подразделениями и офисами банков, банком и процессинговым центром, процессинговым центром и банкоматами. Выполняются требования законодательства, блокируются уязвимости во взаимодействии в финансовой сфере.

Если рассматривать в качестве примера объекта КИИ банкомат, то там сегодня все устроено на первый взгляд довольно просто. В его составе есть диспенсер (в нем лежат деньги и из него деньги выдаются), компьютер и периферийное оборудование. Компьютер взаимодействует с процессинговым центром (например, по IP-протоколу), и USB-кабелями соединен с диспенсером и другим периферийным оборудованием.

При работе с банкоматом с пластиковой карты считывается ее номер, с клавиатуры – PIN, все это передается в процессинговый центр, где и выполняется авторизация. Если все в порядке – проверяется запрашиваемая сумма. Затем компьютером банкомата формируется команда на выдачу денег, которая передается в диспенсер. Из защитных механизмов здесь используется только один – диспенсер размещен в сейфе.

Такого очень упрощенного описания уже достаточно, чтобы понять «Что делать?». Надо защитить каналы – как от процессингового центра к компьютеру, так и от компьютера к диспенсеру, и обеспечить целостность программно-аппаратной среды компьютера. Сделать это в соответствии с 187-ФЗ, нетравматично для функционирования системы и с сохранением инвестиций можно именно с помощью решения fin-TrusT на платформе специализированного компьютера с аппаратной защитой данных m-TrusT.

Финансовые коммуникации становятся безопасными.

Безопасный транспорт

Представим себе железную дорогу как некоторый обобщенный эталонный макет транспорта вообще.

Если рассматривать ее с точки зрения сетевого взаимодействия объектов КИИ (это лишь одно из большого числа крайне интересных проявлений этого феномена, однако именно ему посвящена эта брошюра), то мы увидим три глобальных типа объектов: подвижные составы, станционное оборудование и некоторый центральный вычислительный центр (ведь мы рассматриваем условную модель, а не конкретную КИИ).

Основное взаимодействие происходит между подвижными составами и центральным

вычислительным центром (назовем его ЦВЦ). Он рассылает расписание, аккумулирует данные от подвижных составов и рассылает сделанные на основании этих данных корректировки. Станционное оборудование также отправляет в ЦВЦ данные о движении подвижных составов и получает корректировки расписания, которые передает подвижным составам, а также выполняет различные вспомогательные функции, прописывать которые на уровне такой контурной обрисовки условной транспортной системы нет смысла. Подвижные составы также параллельно взаимодействуют со станционным оборудованием и с ЦВЦ, отправляя данные о своем движении и получая указания и корректировки. Очевидно, что нарушения этого взаимодействия может иметь крайне неприятные последствия, и так же очевидно, что средства защиты этого взаимодействия должны быть унифицированы, но в то же время адаптированы к работе в совершенно разных условиях. Бортовой компьютер подвижного состава работает в условиях вибрации и нагревания, и в целом он абсолютно не похож на ПК или сервер. На станциях оборудование представляет собой стойку серверов, ЦВЦ – это ЦОД с серверами огромной производительности. То есть это задача для платформы m-TrusT. Реализация СКЗИ на m-TrusT, с одной стороны, не имеет никаких ограничений по работе «навстречу» с реализациями этого же СКЗИ на любых других

платформах, а с другой – позволяет организовать защищенное взаимодействие параллельно по разным каналам. Транспорт становится безопасным.

Умная энергетика

Объекты энергетики рассмотрим на примере электрических подстанций. Это объекты, предназначенные для приема, преобразования и распределения электричества. Многие из них расположены «в чистом поле» – на открытых пространствах, вдалеке от какой-либо инфраструктуры, и функционируют относительно автономно.

Такие объекты неизбежно вызывают повышенный интерес злоумышленников, о чем писал еще А. П. Чехов[6]. Подключение к подстанции с целью решения каких-то бытовых задач, предельно опасна, так как объект не имеет ресурсов, позволяющих различать легальные и нелегальные запросы. Негативный эффект от таких действий не исчерпывается бесконтрольным потреблением электроэнергии. Цифровые подстанции, имеющие в составе управляющего комплекса противоаварийную систему, могут расценить изменение нагрузки как аварию и включить противоаварийную автоматику – в этом

[6] Чехов А. П. Злоумышленник // Полное собрание сочинений и писем в 30-ти томах. Сочинения. Том 4. М., «Наука», 1984.

случае целевые функции подстанции могут быть не выполнены в нужный момент, а к чему конкретно это приведет – зависит от того, в рамках какой инфраструктуры и для чего предназначена данная конкретная электроустановка.

Средство защиты, которое позволит отличать аутентифицированный и гарантированно неизмененный управляющий сигнал от воздействия «народных умельцев», позволит избежать этих негативных событий. Оно может быть построено на платформе m-TrusT. Для этого разработана специальная интерфейсная плата, позволяющая устанавливать м-траст в корпусе под DIN-рейку.

Умное производство

Сетевое взаимодействие технических средств объектов на производстве (классическое АСУТП) характеризуется рядом важных особенностей:

- основной защищаемой информацией является технологическая (обеспечивающая управление технологическими или чувствительно важными процессами), программно-техническая (программы системного и прикладного характера, обеспечивающие функционирование системы), командная (управляющая) и измерительная информация;

- предъявляются жесткие требования к времени и порядку выполнения автоматизированных функций;

- во взаимодействие включены разнородные, территориально и пространственно распределенные элементы, в которых реализуются разнообразные информационные технологии, это взаимодействие предельно далеко от документооборота на офисных ПК;

- крайне нежелательны отключения систем для проведения мероприятий по обеспечению безопасности информации;

- крайне опасны последствия вывода из строя и (или) нарушения функционирования системы (и здесь уже речь идет об опасности для жизни и здоровья, а не просто ущерб каким-либо интересам большого числа граждан).

Большая часть этих особенностей определяет по существу лишь одно требование общего характера к используемым СЗИ – они должны создаваться с повышенным вниманием к качеству на всех этапах – от проектирования для производства. Как правило, гарантия особенно высокого качества связана с более высокой ценой продукта, а значит, данный сегмент должен быть крайне привлекательным для производителя, что, в свою очередь, обеспечит конкуренцию, та повысит общий уровень качества и т. д.

Однако, иметь в своей продуктовой линейке варианты исполнения СЗИ с огромным разнообразием интерфейсов, в том числе довольно экзотических, производителю сложно и не выгодно, ведь

многотысячные продажи делают стандартные интерфейсы, свойственные офисным компьютерам. Аналогично обстоит дело с форматами данных, с файловыми системами, с поддержкой подключаемого оборудования. Поэтому эксплуатирующая или подрядная организация при создании проекта подсистемы защиты информации вынуждена использовать то, что есть, и за ту цену, которую назначит подчас единственных поставщик, а не то, что соответствует высоким требованиям к качеству, надежности и живучести.

Однако и это еще не все. Особенность многих производств сегодня состоит еще в одном очень существенном обстоятельстве: их управляющие инфраструктурные элементы находятся за рубежом. А это означает, что при неблагоприятных внешнеполитических обстоятельствах эти элементы могут стать рычагами управления не только производственными процессами. Система безопасности таких объектов должна строится в предположении, что центр управления может перестать быть доверенным источником, и его команды должны интеллектуально обрабатываться, а не просто без искажений передаваться на исполнение.

На платформе специализированного компьютера с аппаратной защитой данных m-TrusT можно построить такую систему.

Умный учет

Приборы учета всегда представляли собой цель для «улучшений» как со стороны недобросовестных пользователей учитываемых ресурсов, так и со стороны недобросовестных взимателей платы за эти ресурсы. Самого разного рода «скручивания» и «накручивания» самого разного рода счетчиков возникло, вероятно, одновременно с самими счетчиками. Каждый, то брал в аренду автомобиль, который надо вернуть «с тем же количеством топлива», наверняка замечал, что датчик топлива ведет себя удивительно, а Интернет полнится советами по обходу любых счетчиков – от воды до трафика.

«Умные» приборы учета имеют два существенных отличия:

1) ими можно управлять удаленно, без непосредственного «личного» контакта с каждым, и

2) они несут в себе функциональность не только непосредственно учета, но и управления.

Это совершенно логично – закончился лимит, превышена просрочка по оплате, или наступило еще какое-то заранее назначенное граничным событие – и в установленном порядке отключается подача того, использование чего считает «умный» счетчик. Никакого произвола или человеческого фактора.

За исключением того, что подать эту команду может хакер. А учитывая природу учитываемых

ресурсов, трудно преувеличить общественную значимость ситуации, которую сможет создать злоумышленник, буде в его планах резкое повышение уровня социальной напряженности.

Сделать «умный» учет безопасным можно за счет использования решений на платформе m-TrusT.

Защищенный бизнес

В защите нуждаются не только КИИ. Потребность в защите собственной информационной инфраструктуры, даже если она не является критической с точки зрения государства, все более осознана бизнесом – и уже не только крупным. И для таких информационных систем особенно важным становится баланс цены и качества. Создавая систему защиты «для себя», одинаково неверно переплачивать за правильное название (с какой бы точки зрения «правильным» оно ни было бы) и избыточную функциональность, ни покупать за небольшие деньги ненадежную защиту.

Криптомаршрутизаторы объектового уровня на платформе m-TrusT могут стать как раз тем решением, которое необходимо бизнесу – одного устройства будет достаточно на небольшой офис, оно не займет места, не требует специальных условий размещения и работает прозрачно для пользователей.

ПАТЕНТНОЕ ОПИСАНИЕ

СПЕЦИАЛИЗИРОВАННЫЙ КОМПЬЮТЕР С АППАРАТНОЙ ЗАЩИТОЙ ДАННЫХ

Реферат:

Компьютер содержит недоступный извне механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим Read Only. Задача полезной модели – повышение уровня защищенности со снижением нагрузки на организационно-технические мероприятия – решена тем, что он содержит блок неизвлекаемого ключа, содержащий, в свою очередь, физический датчик случайных чисел (ФДСЧ) и микроконтроллер с внутренней памятью, запрограммированный на исполнение процедур генерации неизвлекаемого ключа подписи на основе случайной последовательности байт, полученных с ФДСЧ, его записи во внутреннюю память, вычисление ключа проверки подписи, соответствующего неизвлекаемому ключу, выработки сессионного ключа на основе случайной последовательности байт, полученных с ФДСЧ, выработки ключа защиты ключей на основании ранее выработанных неизвлекаемого ключа подписи и ключа ее проверки, зашифровывания на данном ключе сессионного ключа, а также последующее расшифровывание сессионного ключа на ключе

защиты ключей, выработанном, в свою очередь, на основе неизвлекаемого ключа подписи и ключа ее проверки.

Полезная модель относится к области компьютерной техники и информационных технологий и может быть использована там, где требуются защищенные компьютерные средства ограниченной функциональности, поддерживающие заданные криптографические процедуры, в особенности, электронной подписи (ЭП) – например, в качестве бортовых компьютеров сетей оперативно-технологической связи железнодорожного транспорта.

Можно считать доказанным, что в подобных случаях целесообразно применять компьютеры с аппаратной защитой данных, которая обеспечивает более высокий уровень защищенности – в отличие от программной защиты – по отношению к хакерским атакам. Подобные компьютеры содержат, по меньшей мере, один элемент электрической схемы, управляющий доступом в режиме записи к перепрограммируемому запоминающему устройству, хранящему критичные данные – в частности, специализированную операционную систему [1]. Наиболее близким к полезной модели является компьютер, в котором упомянутый элемент представляет собой недоступный извне

механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим RO (Read Only) [2].

Однако поддержание компьютером криптографических процедур, стандартизованных для подобных применений, требует правильной (т. е. корректной и в то же время простой) организации работы с ключевыми данными – а этот вопрос для известных компьютеров с аппаратной защитой данных до настоящего времени так и не нашел удовлетворительного решения. В частности, в вышеуказанном примере задача работы с ключами шифрования возлагалась бы на машиниста локомотива, в обязанности которого входило бы их периодическое обновление путем подключения к каналам ввода-вывода бортового компьютера съемного носителя ключевой информации. Это повысило бы нагрузку на организационно-технические мероприятия на железнодорожном транспорте и снизило бы уровень защищенности, поскольку эти ключи должны быть генерированы где-то извне, съемный носитель с ними вручен машинисту, который – естественно – должен быть соответствующим образом подготовлен к выполнению таких специальных работ, затем машинист должен доставить носитель до локомотива, и, наконец, произвести процедуру обновления. Не говоря об усложнении учетных и

контрольных операций, на каждый отрезок этой цепочки оказывает негативное влияние человеческий фактор, что является недостатком компьютера, требующего такого порядка работы с ключами.

С другой стороны, в последние годы для криптографических токенов и чипов смарт-карт был предложен и успешно реализован принцип неизвлекаемости ключей, состоящий в том, что ключ шифрования и/или ключ подписи никогда не покидает пределов чипа, внутри которого он был сгенерирован. Это позволяет исключить экспорт ключей, поскольку все внешние функции (запрос на сертификат, проверка ЭП и т.п.) можно исполнить при помощи ключей проверки подписи (открытых ключей) [3].

Задачей полезной модели является повышение уровня защищенности, обеспечиваемого компьютером, и снижение нагрузки на организационно-технические мероприятия. Техническим результатом является получение более простого в эксплуатации и лучше защищенного компьютера.

Указанный результат достигнут раскрываемой ниже аппаратной реализацией принципа неизвлекаемости ключей шифрования, адаптированной к специализированному компьютеру с аппаратной защитой данных.

А именно, в специализированном компьютере с аппаратной защитой данных, содержащем недоступный извне механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим RO, новым является то, что он дополнительно содержит блок неизвлекаемого ключа, содержащий, в свою очередь, физический датчик случайных чисел (ФДСЧ) и микроконтроллер с внутренней памятью, запрограммированный на исполнение следующих процедур:

генерации неизвлекаемого ключа подписи на основе случайной последовательности байт, полученных с ФДСЧ, его записи во внутреннюю память, и вычисление ключа проверки подписи, соответствующего неизвлекаемому ключу;

выработки сессионного ключа на основе случайной последовательности байт, полученных с ФДСЧ, и выработки ключа защиты ключей на основании ранее выработанных неизвлекаемого ключа подписи и ключа ее проверки, и зашифровывания на данном ключе сессионного ключа;

расшифровывание сессионного ключа на ключе защиты ключей, выработанном, в свою очередь, на основе неизвлекаемого ключа подписи и ключа ее проверки.

Данные отличия обеспечивают достижение указанного результата, поскольку при эксплуатации такого компьютера процедура обновления закрытых ключей, периодически проводимая с участием человека, больше не требуется. Такое решение промышленно применимо, т. к. оно соответствует действующим отечественным и международным нормативам [4, 5].

ИСТОЧНИКИ ИНФОРМАЦИИ

1. Патент России на полезную модель №138562.

2. Патент России на полезную модель №118773.

3. Сабанов А.Г. О неизвлекаемости закрытых ключей. «Защита информации. Инсайд» №2, март-апрель 2015.

4. ГОСТ Р ИСО/МЭК 9594-8-98.

5. ISO/IEC 13888-3:2009.

Формула полезной модели

Специализированный компьютер с аппаратной защитой данных, содержащий недоступный извне механический коммутатор, устанавливающий для запоминающего устройства, хранящего критичные данные, режим Read Only, отличающийся тем, что он содержит блок неизвлекаемого ключа, содержащий, в свою очередь, физический датчик случайных чисел (ФДСЧ) и микроконтроллер с внутренней памятью, запрограммированный на исполнение процедур генерации неизвлекаемого ключа подписи на основе

случайной последовательности байт, полученных с ФДСЧ, его записи во внутреннюю память, вычисление ключа проверки подписи, соответствующего неизвлекаемому ключу, выработки сессионного ключа на основе случайной последовательности байт, полученных с ФДСЧ, выработки ключа защиты ключей на основании ранее выработанных неизвлекаемого ключа подписи и ключа ее проверки, зашифровывания на данном ключе сессионного ключа, а также последующее расшифровывание сессионного ключа на ключе защиты ключей, выработанном, в свою очередь, на основе неизвлекаемого ключа подписи и ключа ее проверки.

КРАТКИЙ ОБЗОР НОРМАТИВНОЙ БАЗЫ ПО КРИТИЧЕСКИМ ИНФОРМАЦИОННЫМ ИНФРАСТРУКТУРАМ

Основные документы

Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 187-ФЗ) [1], вступивший в силу с 1 января 2018 г. регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура, КИИ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Под безопасностью критической информационной инфраструктуры в 187-ФЗ понимается состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак. Под компьютерной атакой понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами

информации. Под объектами критической информационной инфраструктуры понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры (ст. 2, п. 7 187-ФЗ). В свою очередь субъектами критической информационной инфраструктуры являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей (ст. 2, п. 8 187-ФЗ).

Таким образом, 187-ФЗ и его подзаконные акты можно и нужно применять для обеспечения безопасности функционирования систем электронного банкинга.

Рассмотрим основные положения этих документов.

Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [2]. Вводится перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также определяется порядок категорирования этих объектов. Категорирование осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры. Устанавливаются 3 категории значимости. Самая высокая категория – первая, самая низкая – третья. Определен перечень исходных данных для категорирования. Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической

информационной инфраструктуры перечня объектов. Перечень объектов в течение 5 рабочих дней после утверждения направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры (ФСТЭК России). Определен перечень сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости (либо об отсутствии необходимости присвоения ему одной из таких категорий), направляемых в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры. Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий утверждена **приказом ФСТЭК России от 22 декабря 2017 г. № 236** [3].

Следует отметить, что проект данного постановления Правительства Российской Федерации был согласован с Центральным Банком Российской Федерации.

По информации ФСТЭК России в настоящее время насчитывается более 250 систем банковской сферы и иных сфер финансового рынка, подлежащих категорированию в качестве объектов критической

информационной инфраструктуры. Как минимум половина из этих систем так или иначе относится к системам электронного банкинга, и доля их будет только увеличиваться.

Основными проблемными вопросами категорирования, с которыми приходится сталкиваться субъекту критической информационной инфраструктуры, являются:

- определение принадлежности к субъектам критической информационной инфраструктуры;
- определение критических процессов;
- определение перечня объектов критической информационной инфраструктуры, подлежащих категорированию;
- определение необходимости согласования перечня объектов критической информационной инфраструктуры с государственным органом или российским юридическим лицом;
- подготовка сведений о результатах категорирования объектов критической информационной инфраструктуры.

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования утверждены **приказом ФСТЭК России от 21 декабря 2017 г. № 235** [4]. Документ определяет требования к силам, программным и программно-аппаратным средствам обеспечения

безопасности значимых объектов критической информационной инфраструктуры, к организационно-распорядительным документам, к функционированию системы безопасности в части организации работ.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры утверждены **приказом ФСТЭК России от 25 декабря 2017 г. № 239** [5]. Документом в зависимости от категории значимости и угроз безопасности информации определены следующие организационные и технические меры, подлежащие реализации:

идентификация и аутентификация;

управление доступом;

ограничение программной среды;

защита машинных носителей информации;

аудит безопасности;

антивирусная защита;

предотвращение вторжений (компьютерных атак);

обеспечение целостности;

обеспечение доступности;

защита технических средств и систем;

защита информационной (автоматизированной) системы и

ее компонентов;

планирование мероприятий по обеспечению безопасности;

управление конфигурацией;

управление обновлениями программного обеспечения;

реагирование на инциденты информационной безопасности;

обеспечение действий в нештатных (непредвиденных) ситуациях;

информирование и обучение персонала.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации средств защиты информации (это 6 видов средств защиты: межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки,

средства контроля съемных машинных носителей информации, операционные системы):

а) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;

б) в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;

в) в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 категории значимости применяются сертифицированные средства защиты информации, соответствующие (вместо 4-го уровня НДВ) 4 или более высокому уровню доверия. В значимых объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В значимых объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

В случае если значимый объект является государственной информационной системой или информационной системой персональных данных,

меры по обеспечению безопасности значимого объекта и меры защиты информации (персональных данных) принимаются в соответствии с более высокой категорией значимости, классом защищенности или уровнем защищенности персональных данных.

Таким образом, объекты КИИ (автоматизированные и информационные системы в их составе) подлежат защите также, как ГИС и ИСПДн *высоких классов защищенности.*

Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» [6]. Правилами устанавливается порядок осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и его территориальными органами мероприятий по государственному контролю в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Государственный контроль осуществляется путём проведения плановых и внеплановых выездных проверок. Проверка проводится должностными лицами органа государственного контроля, которые указаны в приказе

органа государственного контроля о проведении проверки. Срок проведения плановой проверки не должен превышать 20 рабочих дней. Срок проведения внеплановой проверки не должен превышать 10 рабочих дней. Информация об организации проверок, в том числе об их планировании, о проведении и результатах таких проверок, в органы прокуратуры не направляется, за исключением информации о результатах проверок, проведённых на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Другие документы

Необходимо упомянуть также еще ряд документов ФСТЭК России и ФСБ России.

Приказ ФСТЭК России от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [7].

Приказ ФСТЭК России от 11.12.2017 №229 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской

Федерации» [8]. Содержание этих документов очевидно из названий.

Приказ ФСБ России от 24 июля 2018 г. N 366 «О Национальном координационном центре по компьютерным инцидентам» [9]. Инициирует создание Национального координационного центра по компьютерным инцидентам (НКЦКИ), определяет его задачи и права.

Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации...» [10]. Устанавливает набор параметров инцидентов для передачи в НКЦКИ (не позднее 24 часов с момента их обнаружения) и способы передачи информации.

Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...» [11]. Определяет способы передачи информации об инциденте другим субъектам КИИ и получения сведений субъектами КИИ об атаках. Обмен информацией с иностранными организациями осуществляет НКЦКИ.

Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» [12]. Определяет требования к функциональным возможностям и характеристикам технических средств, необходимых для решения задач центров ГосСОПКА.

Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты...» [13]. Обязывает субъекта КИИ согласовывать с НКЦКИ установку средств ГосСОПКА и уведомлять о приеме их в эксплуатацию. Определяет необходимые для согласования сведения. Срок согласования — до 45 календарных дней.

Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак...» [14]. Определяет состав плана реагирования на инциденты и принятия мер по ликвидации последствий, разрабатываемого субъектом КИИ. Обязует информировать НКЦКИ о результатах реагирования и ликвидации последствий не позднее 48 часов после завершения мероприятий.

Федеральным законом от 26.07.2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"» [15] внесены изменения, предусматривающие ответственность физических и юридических лиц:

создание, распространение и (или) использование ПО или иной компьютерной информации для неправомерного воздействия на КИИ:

- принудительные работы до 5 лет / лишение свободы до 5 лет / штраф до 1 млн руб.

Неправомерный доступ к информации КИИ, если он повлёк вред:

- принудительные работы до 5 лет / лишение свободы до 6 лет / штраф до 1 млн руб.

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом информации КИИ либо правил доступа, если оно повлекло причинение вреда для КИИ:

- принудительные работы до 5 лет / лишение свободы до 6 лет / запрет занимать должности до 3 лет.

Группой лиц или с использованием служебного положения:

- лишение свободы до 8 лет / запрет занимать должности до 3 лет.

Если повлекло тяжкие последствия:

- лишение свободы до 10 лет / запрет занимать должности до 5 лет.

К счастью, специалисты «на местах» не предоставлены сами себе в этой ситуации, в различных учебных центрах и центрах повышения квалификации проводятся курсы повышения квалификации по программам [16], разработанным в соответствии с **«Методическими рекомендациями по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации»** [17], утвержденными ФСТЭК России 16 апреля 2018 г., и примерной программой повышения квалификации **«Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»** [18], утвержденной ФСТЭК России 17 декабря 2018 г. Разработка программы в соответствии с приведенными документами от ФСТЭК означает, что все положения, модули и темы программы утверждены регуляторами, и соответствуют нормативной методической базе.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

3. Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (в ред. Приказа ФСТЭК России от 21 марта 2019 г. № 59) [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (дата обращения: 16.08.2019).

4. Приказ ФСТЭК России от 11 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

5. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60) [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 16.08.2019).

6. Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной

инфраструктуры» [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/287-postanovleniya/1617-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-17-fevralya-2018-g-n-163 (дата обращения: 20.08.2019).

7. Приказ ФСТЭК России от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227 (дата обращения: 16.08.2019).

8. Приказ ФСТЭК России от 11.12.2017 №229 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1475-prikaz-fstek-rossii-ot-11-dekabrya-2017-g-n-229 (дата обращения: 16.08.2019).

9. Приказ ФСБ России от 24 июля 2018 г. N 366 «О Национальном координационном центре по компьютерным инцидентам» [электронный ресурс]. URL: http://base.garant.ru/72041506/ (дата обращения: 16.08.2019).

10. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [электронный ресурс]. URL: http://base.garant.ru/72041504/ (дата обращения: 16.08.2019).

11. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской

Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» [электронный ресурс]. URL: http://base.garant.ru/72041500/ (дата обращения: 16.08.2019).

12. Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» [электронный ресурс]. URL: http://base.garant.ru/72257648/ (дата обращения: 16.08.2019).

13. Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=329209&fld=134&dst=1000000001,0&rnd=0.3852266461376137#02990060554834295 (дата обращения: 20.08.2019).

14. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=329210&fld=134&dst=1000000001,0&rnd=0.9251330703791609#06741709231220478 (дата обращения: 20.08.2019).

15. Федеральный закон от 26.07.2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» [электронный ресурс]. URL: https://rg.ru/2017/07/31/uk-dok.html (дата обращения: 16.08.2019).

16. Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры [электронный ресурс]. URL: http://www.okbsapr.ru/pclass-6.html (дата обращения: 24.09.2019).

17. Информационное сообщение ФСТЭК России от 23 апреля 2018 г. N 240/11/1868 «О разработанных ФСТЭК России Методических рекомендациях по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации» от 23 апреля 2018 г. N 240/11/1868 [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/1559-informatsionnoe-soobshchenie-fstek-rossii-ot-23-aprelya-2018-g-n-240-11-1868 (дата обращения: 16.08.2019).

18. Информационное сообщение ФСТЭК России от 17 декабря 2018 г. N 240/11/5453 «О разработанной ФСТЭК России примерной программе повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/1761-informatsionnoe-soobshchenie-fstek-rossii-ot-17-dekabrya-2018-g-n-240-11-5453 (дата обращения: 16.08.2019).