Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Кафедра Конструирования и производства радиоэлектронных средств

Дисциплина: «САПР технологических процессов производства электронных средств»

ТЕМА 8: Основы защиты информации в САПР

Лекция № 13. Программные и технические средства защиты информации в САПР

(2 часа)

Доцент кафедры, к.п.н.,

Мордовин В.Н.

2018 г.

СПб ГУТ)))

Учебные вопросы

1. **Аппаратно-программный модуль доверенной загрузки (АПМДЗ).**

1.1. Назначение изделия.

1.2. Состав изделия.

1.3. Технические характеристики и устройство АПМДЗ.

1.4. Основные принципы функционирования АПМДЗ.

2. Система Secret Net.

2.1. Назначение, основные функции и состав системы Secret Net.

2.2. Архитектура и средства управления.

2.3. Сетевая структура системы Secret Net.

Литература

1. Средство защиты информации SECRET NET 7. Руководство администратора. Принципы построения. © Компания "Код Безопасности", 2017.

2. Система обмена информацией в электронном виде вооруженных сил российской федерации.: Учеб. пособие / Под ред. О. В. Рисмана. – СПб.: ВАС, 2011.

ВВЕДЕНИЕ

В настоящее время в РФ научно-теоретической основой для разработки требований к построению систем защиты информации и защищенных вычислительных систем является «***Концепция защиты СВТ и АС от НСД к информации***». Основные положения Концепции заключаются в следующих ***принципах***:

Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

1. Аппаратно-программный модуль доверенной загрузки (АПМДЗ)

1.1. Назначение изделия

- ***Аппаратно-программный модуль доверенной загрузки (АПМДЗ) предназначен для контроля доступа к ПЭВМ, контроля целостности операционной системы (ОС), программного обеспечения (ПО) и данных пользователя и блокировки загрузки нештатной ОС.***

На российском рынке информационной безопасности можно *встретить следующие изделия*:

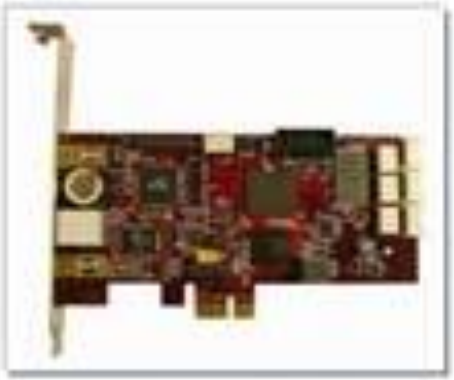
• ***программно-аппаратные комплексы (ПАК) семейства "Соболь"*** разработки "Код Безопасности";

• ***ПАК средств защиты информации от несанкционированного доступа (СЗИ НСД)*** семейства "Аккорд-АМДЗ";

- ***АПМДЗ семейства "Криптон-Замок"*** – фирмы "Анкад";
- ***АПМДЗ "Максим"*** – "НПО "РусБИТех"***;***
- ***АПМДЗ семейства "Цезарь"*** – Всероссийского НИИ автоматизации управления в непромышленной сфере им. В. В. Соломатина;
- ***аппаратный модуль Diamond ACS HW в составе средства контроля и разграничения доступа Diamond ACS*** – *"ТСС".*

Внешний вид плат АМПДЗ.

ПАК «Соболь»



АМДЗ Аккорд-5.5.е

АПМДЗ «КРИПТОН-ЗАМОК»

В данном вопросе лекции будут рассмотрены основные возможности и характеристик АПМДЗ на примере устройств семейства "Цезарь".

Аппаратно-программный модуль доверенной загрузки *представляет собой комплект программно-аппаратных средств, устанавливаемый на ПЭВМ и обеспечивающий доверенную загрузку операционной системы на ПЭВМ, предназначенную для обработки информации, составляющей Государственную тайну. После тестирования и выполнения ряда настроек (администрирования) АПМДЗ позволяет реализовать на данном ПЭВМ требуемую политику безопасности независимо от программного обеспечения (в том числе и операционной системы), установленного на ПЭВМ.*

1.2. Состав изделия

Рис. 2. Типовой состав АМПДЗ семейства «Соболь».

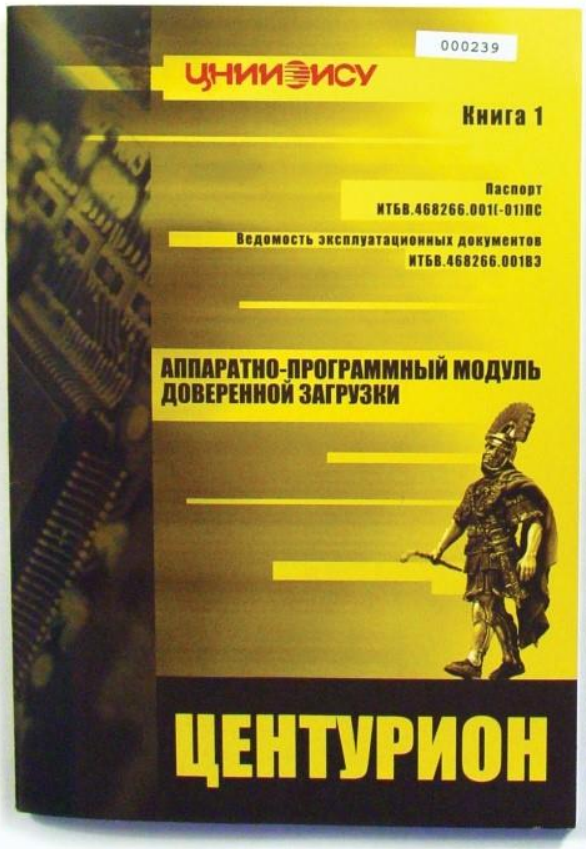
В типовой состав АПМДЗ входят следующие функциональные узлы (см. рис.2):

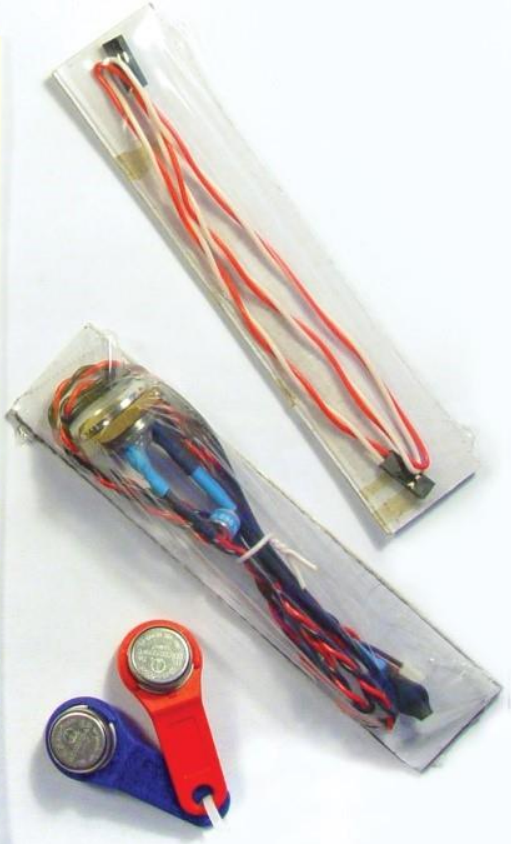
- ***специализированная плата АПМДЗ;***
- ***комплект аутентифицирующих носителей пользователей (АНП);***
- ***устройство подключения АНП;***
- ***управляющий кабель;***
- ***загрузочный (с ОС MS-DOS) компакт-диск с программным обеспечением АПМДЗ, включающий программу инициализации и тестирования АПМДЗ и набор драйверов АПМДЗ;***
- ***эксплуатационная документация.***

Доступ к ПЭВМ с установленным АПМДЗ возможен *только для пользователей, которые прошли регистрацию* на данном АПМДЗ и имеют инициализированные АНП.

Настройка и администрирование АПМДЗ осуществляется *специально выделенным пользователем - администратором* АПМДЗ.

Рис. 3. Типовой состав АМПДЗ семейства «Центурион».





1.3. Технические характеристики и устройство АПМДЗ

Характеристика	Значение
Тип аутентифицирующего носителя пользователя (АНП)	Touch Memory (TM) или Карта РИК-М* (в зависимости от комплектации)
Количество ПЭВМ, на которых может использоваться один АНП	Неограниченно
Длина уникального номера носителя (УНН)	Для Touch Memory (TM) – 64 бита Для карты РИК-М – 32 бита
Длина персонального идентификационного кода (ПИК)	256 бит
Алгоритм аутентификации пользователя	На основе ГОСТ 28147-89
Длина пароля	От 8 до 16 символов
Количество пользователей, допускаемых к ПЭВМ	До 32 (без учета администратора)
Поддерживаемые ОС	ОС МСВС 3.0, ЗОС «Оливия»
Контролируемые интерфейсы ПЭВМ	Производится контроль всех интерфейсов ПЭВМ, с которых поддерживается загрузка ОС в системном BIOS

Рис. 5. Внешний вид платы АМПДЗ «Цезарь».

- **Рис. 4. Внешний вид платы АМПД3 типа «Криптон».**

Специализированная плата АПМДЗ функционально состоит из следующих узлов:

- интерфейс шины PCI;
- узел технологической перемычки;
- аппаратный таймер;
- узел формирования сигнала RESET;
- датчик случайных чисел (ДСЧ);
- память для хранения программы АПМДЗ;
- память для хранения кодов прошивки;
- электронный диск объемом 4 Мб, который может использоваться как загрузочный диск (для хранения ядра операционной системы), а также для хранения критичных данных пользователя (данных, которые не должны быть случайно или преднамеренно изменены);
- энергонезависимая память (ЭНП) для хранения конфигурационной служебной информации АПМДЗ;
- часы реального времени с автономным источником питания (миниатюрная литиевая батарея);
- дополнительная ОП, предназначенная для передачи информации от АПМДЗ в программную систему защиты.

1.4. Основные принципы функционирования АПМДЗ

Идентификация и аутентификация. АПМДЗ осуществляет идентификацию пользователя по постоянному *уникальному номеру носителя* (УНН), хранящемуся в АНП и в *энергонезависимой памяти* (ЭНП) платы АПМДЗ (области списка реквизитов администратора и пользователей). Для идентификации пользователь должен предъявить АНП (присоединить ТМ или смарт-карту, в зависимости от комплектации, к специальному считывателю).

В случае несовпадения предъявленного УНН ни с одним из УНН, хранящимся в ЭНП, принимается решение об отрицательном результате идентификации. После идентификации пользователя производится проверка счетчика считываний предъявленного пользователем АНП на данном ПЭВМ за текущие сутки. Если этот счетчик достигнет установленного администратором максимального значения, то аутентифицирующая информация из АНП не считывается и пользователю отказывается в доступе до истечения текущих суток.

Аутентификация пользователя со стороны АПМДЗ осуществляется по следующему алгоритму:

- чтение из памяти АНП *персонального идентификационного кода* (ПИК) и эталона *контрольного вектора носителя* (КВН);
- запрос *пароля* (ПАР) с клавиатуры ПЭВМ;
- вычисление КВН по алгоритму ГОСТ 28147-89 с использованием ПАР и ПИК;
- проверка подлинности ПИК путем сравнения вычисленного значения КВН с эталоном, считанным из АНП (при отрицательном результате проверки подлинности ПИК принимается решение об отрицательном результате аутентификации);

- вычисление контрольного вектора пользователя (КВП) по алгоритму ГОСТ 28147-89 с использованием ПИК (при отрицательном результате сравнения принимается решение об отрицательном результате аутентификации);
- проверка КВП путем сравнения вычисленного значения КВП с эталоном, хранящимся в ЭНП платы АМПДЗ (в случае отрицательного результата идентификации или аутентификации, АПМДЗ увеличивает количество попыток неудачных входов в ПЭВМ (счетчики попыток неудачных входов размещаются в ЭНП платы АПМДЗ), заносит соответствующую запись в журнал регистрации попыток несанкционированного доступа (НСД), хранящийся в ЭНП платы АПМДЗ, и инициирует команду RESET в ПЭВМ).

Контроль конфигурации ПЭВМ.

АПМДЗ предоставляет возможность контроля целостности конфигурации ПЭВМ до загрузки ОС.

Контроль целостности конфигурации ПЭВМ включает в себя:

- контроль CMOS памяти ПЭВМ;
- контроль BIOS расширений (областей памяти);
- контроль загрузочного сектора (MBR) текущего загрузочного диска;
- контроль ESCD (при поддержки BIOS);
- контроль таблицы накопителей, доступных через BIOS.

Контроль целостности программной среды ПЭВМ.

- АПМДЗ дает возможность осуществления контроля целостности групп физических секторов и файлов на жестком диске до загрузки ОС.
- Для реализации контроля целостности загрузчика, ядра и модулей ОС, а также программного обеспечения и данных пользователя соответствующие физические сектора (MBR, BOOT) и файлы должны быть включены в список объектов контроля целостности средствами АПМДЗ.
- Контроль целостности осуществляется средствами программы АПМДЗ по алгоритму ГОСТ 28147-89 с использованием уникального ключа платы (УКП), хранящегося в недоступной для ПЭВМ области ЭНП платы АПМДЗ.
- Факт нарушения целостности программной среды ПЭВМ фиксируется в журнале НСД.

Разграничение доступа.

По результату аутентификации пользователя/ администратора АПМДЗ осуществляет разграничение доступа к ресурсам АПМДЗ и ПЭВМ в соответствии с установленными полномочиями администратора и пользователей:

- разрешение/запрет администрирования;
- разрешение/запрет смены пароля;
- разрешение/запрет смены ПИК;
- разрешение/запрет загрузки штатной версии ОС (штатной считается версия ОС, загружаемая с носителя указанного в настройках АПМДЗ в качестве загрузочного – это может быть накопитель на жестком магнитном диске (НЖМД), встроенный в АПМДЗ электронный диск, последовательность загрузочных носителей (в том числе внешних), указанная в BIOS);

- разрешение/запрет чтения данных со встроенного электронного диска;
- разрешение/запрет записи данных на встроенный электронный диск (доступно только администратору);
- разрешение/запрет загрузки нештатной версии ОС (с любого носителя, отличного от заданных в АПМДЗ в качестве загрузочных);
- разрешение/запрет загрузки ОС при отрицательных результатах контроля целостности ПС ПЭВМ.

С использованием подсистемы разграничения доступа АПМДЗ реализуется следующая *политика безопасности*:

- доступ к администрированию АПМДЗ разрешен администратору только после успешной аутентификации с предъявлением основного или резервного АНП и запрещен для всех пользователей;
- доступ к функции «смена пароля» разрешен как администратору, так и пользователям (самостоятельно без администратора) только после их положительной аутентификации. Для пользователей доступ к функции «смена пароля» может быть запрещен установкой администратором соответствующего флага;
- доступ к функции «смена ПИК» разрешен как администратору, так и пользователям (самостоятельно без администратора) только после их положительной аутентификации. Для пользователей доступ к функции «смена ПИК» может быть запрещен установкой администратором соответствующего флага;

- загрузка штатной ОС разрешается администратору и любому из привилегированных пользователей только в случае их положительной аутентификации;
- загрузка штатной ОС разрешается любому из обычных (непривилегированных) пользователей после их положительной аутентификации, только если целостность контролируемых средствами АПМДЗ объектов ПС ПЭВМ не нарушена;
- загрузка нештатной версии ОС разрешается администратору только после его положительной аутентификации и запрещается всем другим пользователям.

Состояния и режимы функционирования АПМДЗ.

АПМДЗ может находиться в одном из двух состояний: *технологическом или эксплуатационном.*

Технологическое состояние предназначено для тестирования АПМДЗ и подготовки его к инициализации (со сбросом всех настроек). В технологическом состоянии при включении питания ПЭВМ запуск программы АПМДЗ (расширения BIOS) не производится, а тестирование АПМДЗ и подготовка его к инициализации проводится администратором с использованием ПО АПМДЗ, поставляемого на компакт-диске.

В эксплуатационном состоянии АПМДЗ функционирует под управлением программы АПМДЗ.

В эксплуатационном состоянии различается два режима: *режим инициализации и рабочий режим*.

Режим инициализации предназначен для:

• выбора типа используемого АНП и способа его подключения;

• записи в ЭНП платы АПМДЗ конфигурационных параметров, реквизитов администратора;

• сброса (установки в нуль) счетчиков в журнале регистрации попыток НСД;

• записи в АНП администратора всей информации, необходимой для администрирования АПМДЗ и работы администратора на ПЭВМ.

Рабочий *режим АПМДЗ является основным.* В этом режиме после выполнения инициализации АПМДЗ выполняет свои функции, обеспечивая доверенную загрузку ОС.

Для защиты от обхода запуска программы АПМДЗ на плате предусмотрен аппаратный таймер, который в процессе своего функционирования независимо от выполняемой ПЭВМ программы может инициировать выдачу сигнала RESET от платы АПМДЗ в ПЭВМ.

2. Система Secret Net

Система Secret Net предназначена для защиты от несанкционированного доступа к информационным ресурсам компьютеров, функционирующих под управлением операционных систем MS Windows 8/7/Vista/XP и Windows Server 2012/2008/2003.

Защита от несанкционированного доступа (НСД) обеспечивается комплексным применением набора защитных механизмов, расширяющих средства безопасности ОС Windows.

Система может функционировать в следующих *режимах*:

- ***автономный*** режим — предусматривает только локальное управление защитными механизмами;
- ***сетевой*** режим — предусматривает локальное и централизованное управление защитными механизмами, а также централизованное получение информации и изменение состояния защищаемых компьютеров.

Основные функции, реализуемые системой Secret Net:

• контроль входа пользователей в систему;

• разграничение доступа пользователей к ресурсам файловой системы и устройствам компьютера;

• создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды);

• разграничение доступа пользователей к конфиденциальным данным;

• контроль потоков конфиденциальной информации в системе;

• контроль вывода на печать и добавление грифов в распечатываемые документы (маркировка документов);

• контроль целостности защищаемых ресурсов;

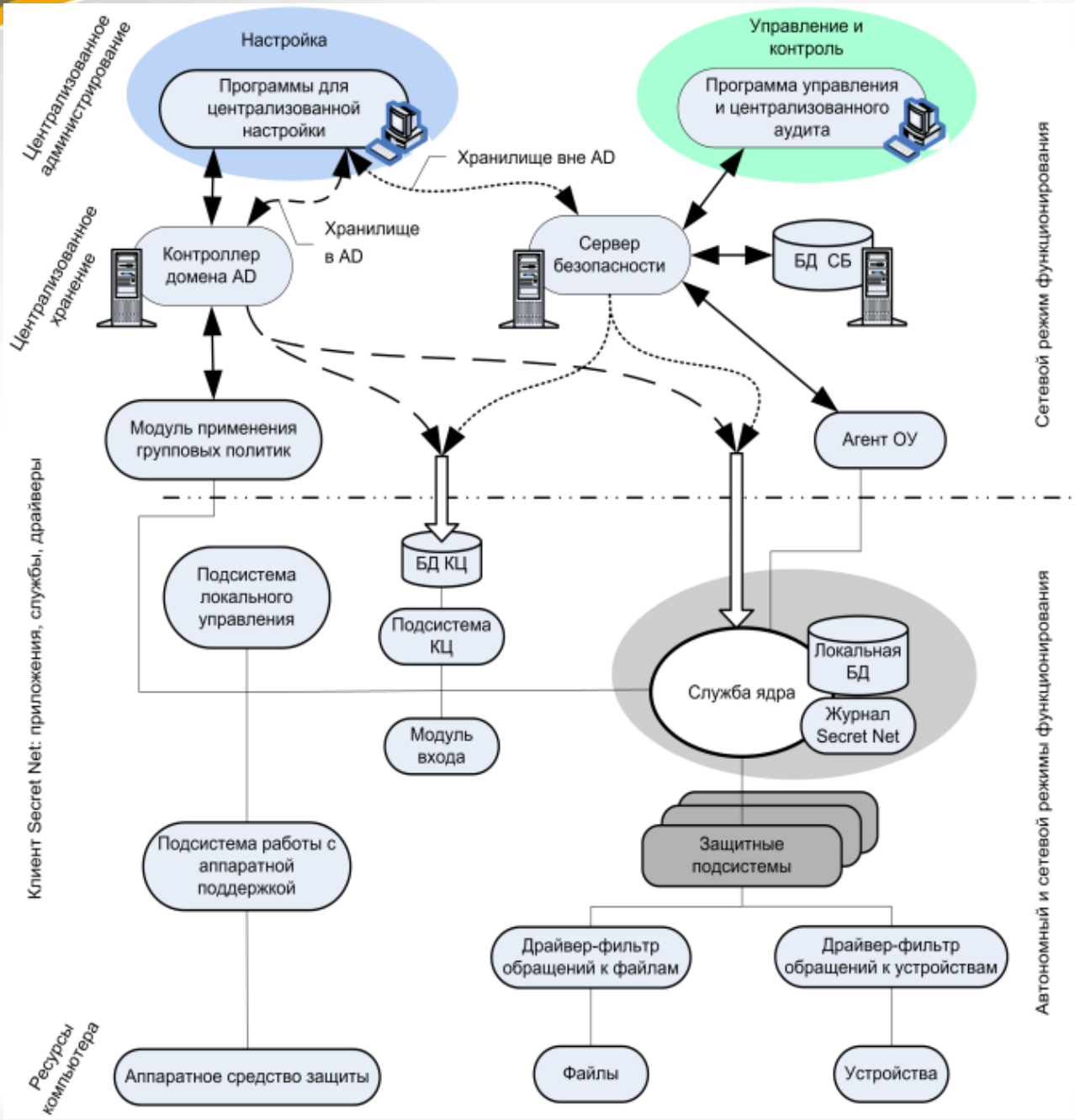
• контроль подключения и изменения устройств компьютера;
• функциональный контроль ключевых компонентов SecretNet;
• защита содержимого дисков при несанкционированной загрузке;
• уничтожение (затирание) содержимого файлов при их удалении;
• теневое копирование выводимой информации;
• регистрация событий безопасности в журнале Secret Net;
• мониторинг и оперативное управление защищаемыми компьютерами (только в сетевом режиме функционирования);
• централизованный сбор и хранение журналов (только в сетевом режиме функционирования);
• централизованное управление параметрами механизмов защиты (только в сетевом режиме функционирования).

Состав устанавливаемых компонентов.

Система Secret Net состоит из следующих отдельно устанавливаемых программных средств:

1. Компонент "***Secret Net 7***" (клиент).
2. Компонент "***Модификатор схемы Active Directory***" (модификатор AD). Используется только в сетевом режиме функционирования. Применяется в случае использования Active Directory для размещения и хранения сведений об объектах централизованного управления.
3. Компонент "***Secret Net 7 — Сервер безопасности***" (сервер безопасности или СБ). Используется только в сетевом режиме функционирования.
4. Компонент "***Secret Net 7 — Программа управления***" (программа оперативного управления). Используется только в сетевом режиме функционирования.

2.2. Архитектура и средства управления



Основные подсистемы клиента Secret Net Клиент включает следующие основные компоненты и подсистемы:

- служба ядра;
- подсистема локального управления;
- защитные подсистемы;
- модуль входа;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой.

Служба ядра автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера.
Она осуществляет управление подсистемами и компонентами и обеспечивает их взаимодействие.

Подсистема локального управления обеспечивает:

• управление объектами защиты (устройствами, файлами, каталогами);

• управление параметрами пользователей и защитных механизмов;

• взаимодействие с локальной БД Secret Net;

• формирование заданий на контроль целостности;

• просмотр локальных журналов.

Защитные подсистемы:

• Замкнутая программная среда.

• Затирание данных.

• Защита дисков.

• Разграничение доступа к устройствам.

• Теневое копирование.

• Полномочное управление доступом.

• Контроль печати.

• Дискреционное управление доступом.

Модуль входа совместно с ОС Windows обеспечивает:

- обработку входа пользователя в систему (проверка возможности входа, оповещение остальных модулей о начале или завершении работы пользователя);
- блокировку работы пользователя;
- функциональный контроль работоспособности системы;
- загрузку данных с персональных идентификаторов пользователя;
- усиленную аутентификацию пользователя при входе в систему.

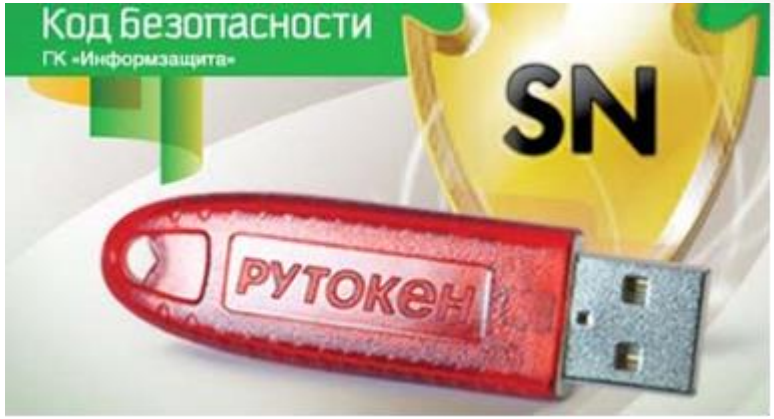


Рис.7. Вид ключа безопасности системы.

При обработке входа пользователя в систему осуществляется формирование контекста пользователя: определение его привилегий, уровня допуска и др.

Подсистема контроля целостности обеспечивает проверку неизменности ресурсов (каталогов, файлов, ключей и значений реестра) компьютера. Хотя данная подсистема и выполняет контролирующие функции, она *не включена в состав защитных подсистем, так как выполняет контроль не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе* (загрузка, вход пользователя, контроль по расписанию).

Подсистема работы с аппаратной поддержкой обеспечивает взаимодействие с устройствами аппаратной поддержки системы Secret Net и состоит из следующих компонентов:

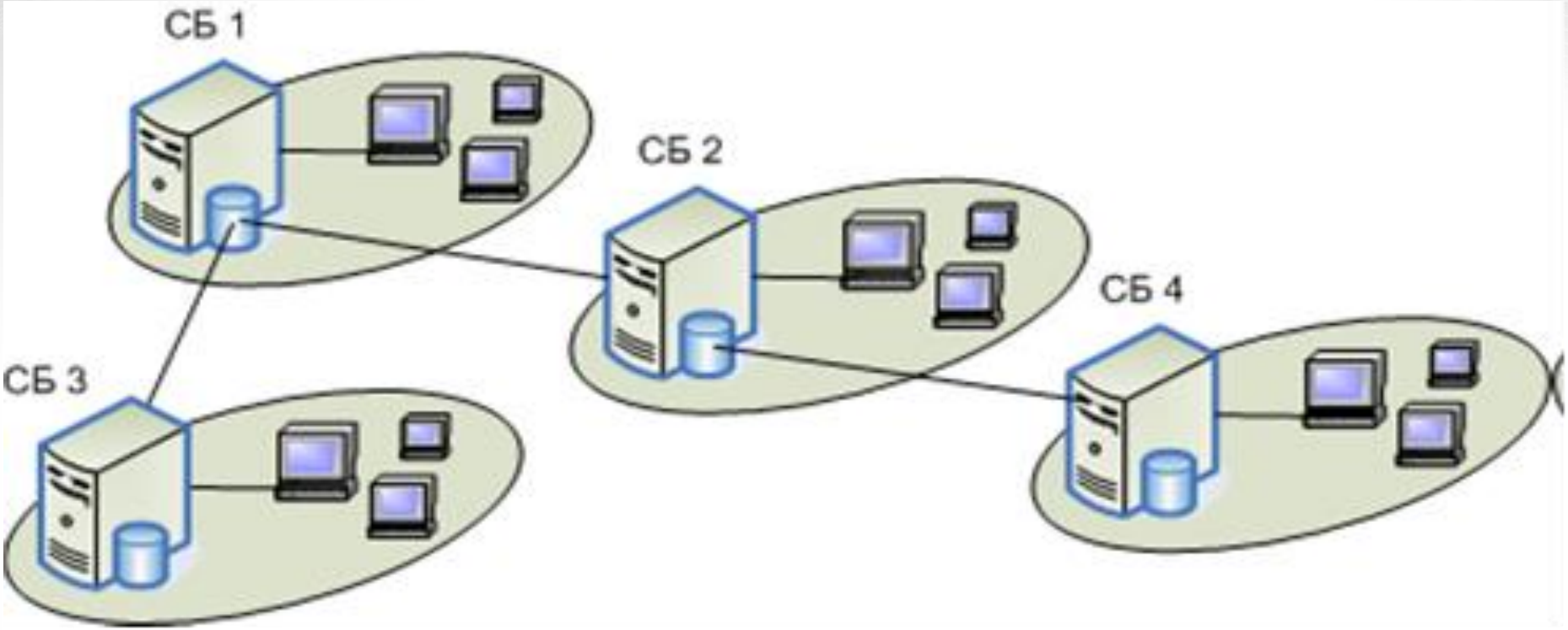
- модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам;
- модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
- драйверы устройств аппаратной поддержки (если они необходимы).

2.3. Сетевая структура системы Secret Net

Для централизованного управления в ***сетевом режиме в*** системе должны быть установлены следующие программные средства:

- ***компонент "Secret Net 7 — Сервер безопасности".***
- ***компонент "Secret Net 7"*** *в сетевом режиме* функционирования — на всех защищаемых компьютерах.
- ***компонент "Secret Net 7 — Программа управления"*** — на рабочих местах администраторов, в задачи которых входит конфигурирование сетевой структуры системы Secret Net, мониторинг, оперативное управление или работа с централизованными журналами.
- В сетевом режиме функционирования предоставляются возможности централизованного управления, мониторинга и получения локальных журналов для компьютеров, ***функционирующих под управлением ОС семейства Linux***.

Пример использования нескольких серверов безопасности



Сетевая структура системы Secret Net строится по принципу подчинения защищаемых компьютеров сети серверу безопасности. Для подчинения серверу безопасности компьютер должен быть в составе домена безопасности.

Сетевую структуру системы Secret Net можно формировать с учетом различных особенностей построения сети и распределения полномочий между администраторами.

Заключение

Перечень принятых сокращений при работе с АПМДЗ

АНП	аутентифицирующий носитель пользователя.
АПМДЗ	аппаратно-программный модуль доверенной загрузки.
ДСЧ	датчик случайных чисел.
КВН	контрольный вектор носителя.
КВП	контрольный вектор пользователя.
МОЧ	максимальное число отказов.
МПЧ	максимальное число попыток.
НЖМД	накопитель на жестком магнитном диске.
НСД	несанкционированный доступ.
ОКП	общий ключ платы.
ОС	операционная система.
ПАР	Пароль.
ПИК	персональный идентификационный код.
ПЛИС	программируемая логическая интегральная схема.
ПО	программное обеспечение.
ПС	программная среда.
ПСЗИ	программная система защиты информации.
РС	рабочая станция.
СНВ	счетчик неудачных попыток входа пользователя.
СНП	счетчик несанкционированных попыток подбора парольной информации администратора.
СОП	счетчик общего числа попыток НСД.
УЗ	учетная запись.
УКП	уникальный ключ платы.
УНН	уникальный номер АНП.
УПАНП	устройство подключения АНП.
ЭНП	энергонезависимая память.
BIOS	Basic Input Output System (базовая система ввода-вывода).
TM	устройство сенсорной памяти Touch Memory.