ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»

Кафедра Конструирования и производства радиоэлектронных средств_

Утверждаю
Заведующий кафедрой
к.т.н., доцент

«____» _____ 201 года

ЛЕКЦИЯ

по дисциплине «САПР технологических процессов производства электронных средств»

Тема № 5 Основы защиты информации в САПР ТПП

Занятие № 13 Программно-технические средства защиты информации САПР ТПП

Обсуждена на заседании кафедры
Протокол № ___ от
«____» _____ 201 года

Санкт-Петербург
2018

I. Учебные цели

1. Изучить программные и технические средства защиты информации в автоматизированных системах управления предприятием (производством).
2. Ознакомить студентов с особенностями построения и систем защиты информации.

II. Воспитательные цели

1. Воспитание чувства ответственности за качественное освоение изучаемой дисциплины.
2. Поднять творческую составляющую обучения.

III. Расчет учебного времени

Содержание и порядок проведения лекции	Время, мин
Вступительная часть. Основная часть (текст лекции) Учебные вопросы: 1. Аппаратно-программный модуль доверенной загрузки. 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.	3
Заключительная часть	2

IV. 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.
3.

V. Учебно-материальное обеспечение

Наглядные пособия (схемы):

1. Наглядные пособия: Слайды.
2. ТСО: ПЭВМ, мультимедиа-проектор

VI. Текст лекции

Введение

Руководящими документами Гостехкомиссии РФ несанкционированный доступ определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС) (под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС).

В настоящее время в Российской Федерации 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» (Руководящий документ ГТК РФ). 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).

Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

1. Аппаратно-программный модуль доверенной загрузки

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".

На рисунке 1 представлены некоторые из перечисленных устройств.

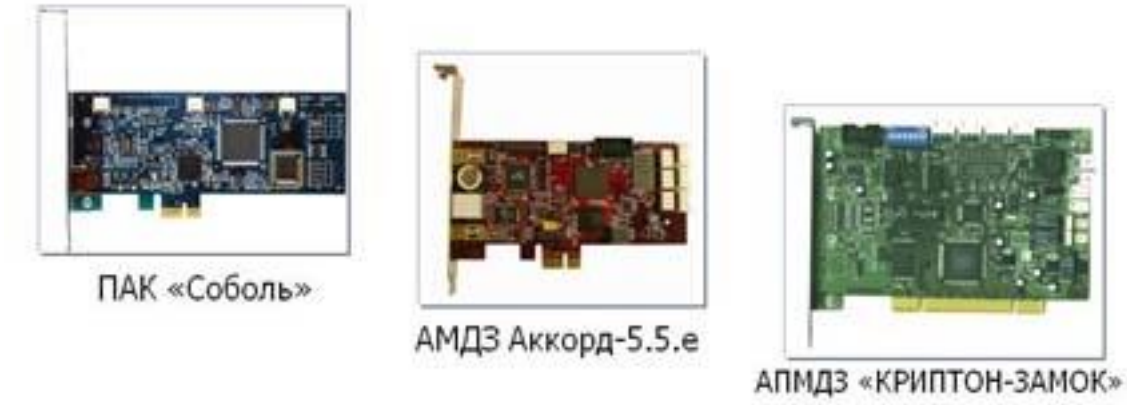

Рис. 1. Внешний вид плат АМПДЗ.

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.

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

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.

1.3. Технические характеристики и устройство АПМДЗ

Технические характеристики АПМДЗ Цезарь» представлены в табл. 1.

Таблица 1

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

Главным функциональным компонентом АПМДЗ является плата расширения в стандарте PCI (рис. 4, 5), вставляемая и свободный слот системной платы ПЭВМ.

Рис. 4. Внешний вид платы АМПДЗ типа «Криптон».

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

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 оперативная память, 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 срав-нения 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).

В случае отказа в запуске по причине отрицательного результата аутентификации АПМДЗ предоставляет пользователю *несколько повторных попыток* ввода. В случае превышения пользователем предельного числа попыток запуска ПЭВМ работа пользователя блокируется. Дальнейшая работа заблокированного пользователя становится возможна только после снятия блокировки администратором АПМДЗ.

В случае превышения суммы неудачных попыток запуска ПЭВМ всеми пользователями предельного общего числа неудачных попыток запуска ПЭВМ работа всех пользователей блокируется средствами АПМДЗ. Разблокирование пользователей становится возможным только после обнуления администратором счетчика общего числа неудачных попыток.

В случае положительного результата идентификации/аутентификации АПМДЗ сравнивает сроки действия пароля пользователя и ПИК, считываемые из АНП одновременно с УНН, ПИК, КВН и т.д. с текущей датой, полученной из собственных часов реального времени. При истечении одного или обоих сроков действия АПМДЗ работает в соответствии с настроенной реакцией на это событие. АПМДЗ может выдать предупреждение о скором истечении срока действия, потребовать немедленной смены пароля или ПИК или заблокировать пользователя до вмешательства администратора.

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.

В случае *обнаружения каких-либо отклонений* контролируемых параметров конфигурации ПЭВМ АПМДЗ запрещает доступ всем пользователям и разрешает доступ только администратору.

Контроль CMOS памяти ПЭВМ предполагает, что при постановке на контроль, значения определенных ячеек сохраняются в энергонезависимой памяти платы АПМДЗ как эталонные и всякий раз при загрузке ПЭВМ выполняется сравнение реального содержимого этих ячеек с эталонными значениями. Выбор ячеек CMOS памяти, подлежащих контролю, настраивается администратором.

Контроль BIOS расширений (областей памяти) заключается в том, что при постановке на контроль содержимого каждой из заданных областей памяти вычисляется имитовставка, которая сохраняется в энергонезависимой памяти платы АПМДЗ как эталонная. Всякий раз при загрузке ПЭВМ средствами АПМДЗ вычисляются имитовставки от содержимого заданных областей памяти, и выполняется их сравнение с эталонными значениями. Всего таких областей может быть до десяти.

Контроль загрузочного сектора (MBR - Master Boot Record) текущего загрузочного диска выполняется после загрузки MBR в ОЗУ ПЭВМ аналогично тому, как выполняется контроль областей памяти, описанный выше. Параметры контролируемой области стандартизованы и не могут быть изменены. Администратор может только включить или выключить контроль загрузочного сектора.

Контроль таблицы Extended System Configuration Data (ESCD), формируемой BIOS, осуществляется только в том случае, если BIOS поддерживает функции чтения его содержимого. Поддержка зависит от версии и фирмы производителя BIOS, используемого в конкретном ПЭВМ. Если необходимые функции не поддерживаются, контроль не производится. Администратор может только включить или выключить контроль ESCD.

Контроль таблицы накопителей, доступных через BIOS, осуществляется сле-

дующим образом. При постановке на контроль, АПМДЗ используя стандартные прерывания BIOS, формирует таблицу доступных устройств, содержащую их параметры. Затем от содержимого таблицы вычисляется имитовставка, которая сохраняется в энергонезависимой памяти платы АПМДЗ как эталонная. Каждый раз при загрузке ПЭВМ аналогичным образом формируется таблица, вычисляется имитовставка и производится сравнение полученного значения с эталонным.

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.

В рабочем режиме всякий раз при успешной идентификации и аутентификации пользователей и администратора до загрузки ОС будет запускаться процедура подсчета имитовставок от служебного файла и описанных в нем объектов контроля целостности и сравнения их с эталонными значениями. При совпадении всех имитовставок загрузка ОС будет разрешена. При несовпадении хотя бы одной имитовставки будет выдано соответствующее сообщение об ошибке, и для обычных пользователей загрузка ОС будет заблокирована. Для администратора и привилегированных пользователей будет выдано предупреждение с возможностью дальнейшей загрузки ОС.

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 вер-сия 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 за-грузочных 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 па-роля» 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.

При первом запуске программы АПМДЗ после подготовки платы АПМДЗ к инициализации и перевода ее из технологического состояния в эксплуатационное, произойдет автоматическая настройка таймера АПМДЗ под конкретную конфигурацию данного ПЭВМ. После настройки при последующих запусках платы АПМДЗ таймер работает в режиме блокировки. При этом если запуск программы АПМДЗ не произошел в течение временного интервала, на который настроен таймер, то в ПЭВМ будет выдан сигнал RESET. Тем самым работа ПЭВМ в обход программы АПМДЗ будет заблокирована.

АПМДЗ может функционировать автономно или совместно с программной системой защиты информации (ПСЗИ). При инициализации платы АПМДЗ автоматически устанавливается режим совместной работы с ПСЗИ. В процессе администрирования администратор может изменять режим работы ЭНП платы АПМДЗ.

Подсистема контроля целостности ПС ПЭВМ в АПМДЗ может быть включена или отключена. При инициализации АПМДЗ автоматически устанавливается режим его работы с отключенной подсистемой контроля целостности ПС. В процессе администрирования администратор может включать или отключать подсистему контроля целостности ПС.

Журнал регистрации попыток НСД. Для обнаружения попыток НСД в АПМДЗ ведется журнал регистрации попыток НСД, который хранится в ЭНП платы АПМДЗ. Журнал доступен для чтения и модификации только администратору. В нем содержится следующая информация: счетчик несанкционированных попыток (СНП) подбора парольной информации администратора; счетчик общего числа попыток (СОП) НСД; записи попыток НСД.

Счетчик несанкционированных попыток подбора парольной информации администратора предназначен для защиты от исследования АПМДЗ злоумышленником путем предъявления АНП администратора. В процессе инициализации платы АПМДЗ этот счетчик автоматически устанавливается в ноль. При каждой неудачной попытке входа с предъявлением АНП администратора значение СНП увеличивается на единицу. При каждой попытке входа значение этого счетчика сравнивается с 1000. После достижения СНП значения СНП=1000 АПМДЗ будет блокировать доступ к ПЭВМ всех пользователей, включая администратора.

Счетчик общего числа попыток НСД предназначен для защиты от исследования АПМДЗ злоумышленником в целях подбора парольной информации какого-либо из пользователей, путем предъявления набора АНП нескольких пользователей. В процессе инициализации платы АПМДЗ этот счетчик автоматически устанавливается в ноль. При каждой попытке входа с предъявлением незарегистрированного АНП либо при неудачной попытке входа с АНП пользователя значение счетчика увеличивается на единицу. При каждой попытке входа пользователя значение этого счетчика сравнивается с максимальным числом отказов. После достижения СОП значения максимального числа отказав, АПМДЗ будет блокировать доступ всех пользователей к ПЭВМ.

Каждая попытка НСД фиксируется в журнале в виде записи, которая содержит следующие поля: время события; дата события; УНН пользователя, при предъявлении АНП которого произошло событие; тип (код) попытки НСД.

2. Система Secret Net

2.1. Назначение, основные функции и состав системы 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 Secret Net 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 Secret Net;
- 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" (далее — клиент).

2. Компонент "Модификатор схемы Active Directory" (далее — 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" (далее — сервер безопасности или СБ). Используется только в сетевом режиме функционирования.

4. Компонент "Secret Net 7 — Программа управления" (далее — программа оперативного управления). Используется только в сетевом режиме функционирования.

2.2. Архитектура и средства управления

Обобщенная структурная схема взаимодействия основных компонентов системы Secret Net представлена на следующем рисунке.

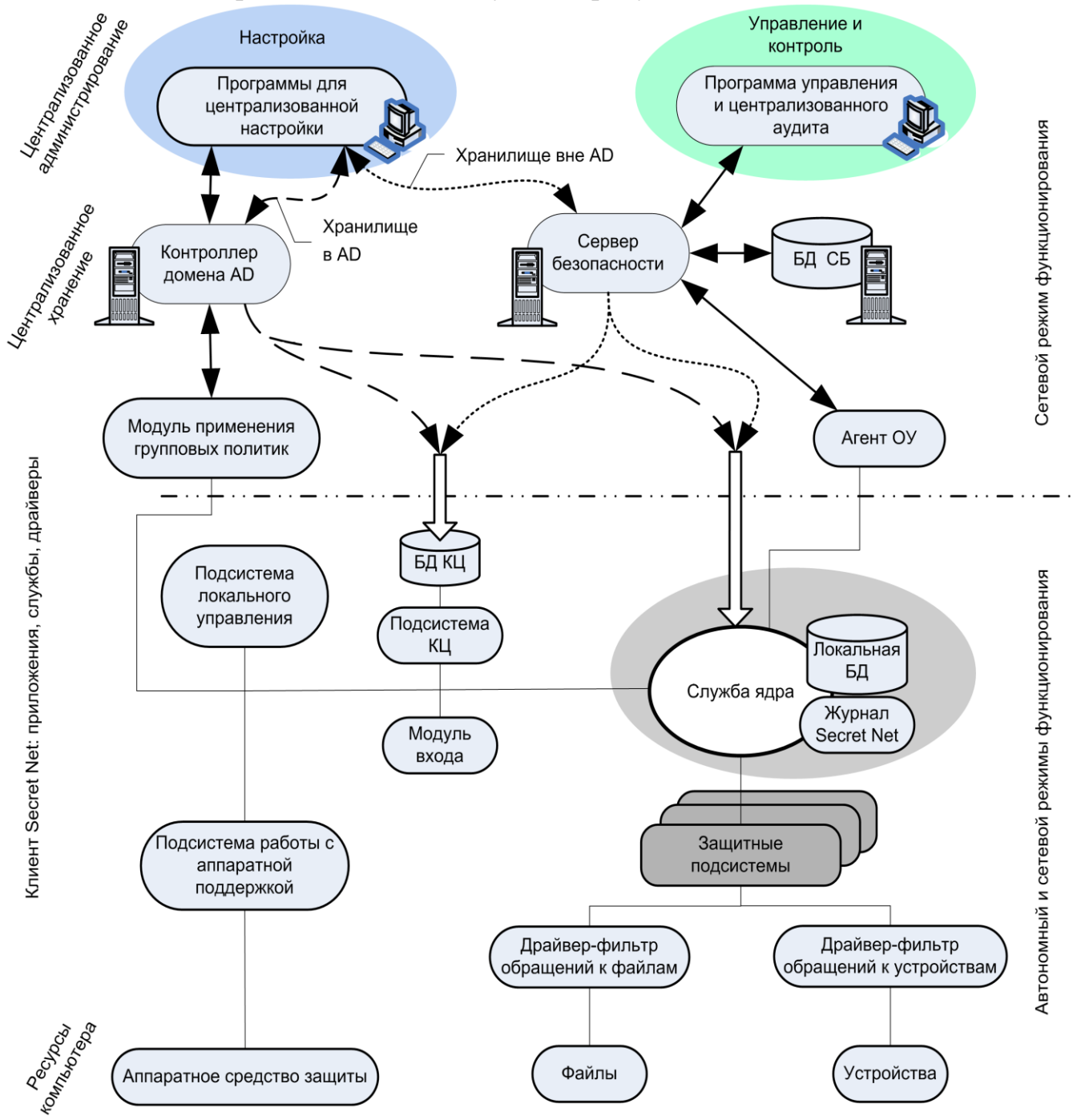

Рис.6. Структурная схема взаимодействия.

Основные подсистемы клиента Secret Net

Клиент системы Secret Net включает следующие основные компоненты и подсистемы:

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

Ядро

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.

Ядро выполняет следующие функции:

- обеспечивает обмен данными между компонентами клиента и обработку поступающих команд;
- обеспечивает доступ других компонентов системы к информации, хранящейся в локальной базе данных Secret Net;
- обрабатывает поступающую информацию о событиях, происходящих на компьютере и связанных с безопасностью системы, и регистрирует их в журнале Secret Net.

Подсистема регистрации является одним из элементов ядра клиента и предназначена для управления регистрацией событий, связанных с работой системы защиты. Такие события регистрируются в журнале Secret Net. Эта информация поступает от подсистем Secret Net, которые следят за происходящими событиями. Перечень событий Secret Net, подлежащих регистрации, устанавливается администратором безопасности.

В локальной БД Secret Net хранится информация о настройках системы защиты, необходимых для работы защищаемого компьютера. Локальная БД размещается в реестре ОС Windows и специальных файлах.

Доступ подсистем и компонентов системы защиты к данным, хранящимся в БД Secret Net, обеспечивается службой ядра.

Подсистема локального управления

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

Со службой ядра взаимодействуют следующие защитные подсистемы:

- *Замкнутая программная среда* — предотвращает запуск неразрешенного программного обеспечения (ПО).
- *Затирание данных* — обеспечивает затирание содержимого удаленных файлов.

- *Защита дисков* — обеспечивает защиту информации на локальных дисках при несанкционированной загрузке компьютера.
- *Разграничение доступа к устройствам* — обеспечивает разграничение доступа к заданным устройствам компьютера (портам, USB- устройствам, локальным дискам и др.).
- *Теневое копирование* — сохраняет в специальном хранилище копии выводимых данных (например, файлов).
- *Полномочное управление доступом* — обеспечивает хранение категорий конфиденциальности ресурсов, разграничение доступа к этим ресурсам и контроль потоков конфиденциальной информации в системе.
- *Контроль печати* — обеспечивает контроль вывода документов на печать (в том числе и конфиденциальных).
- *Дискреционное управление доступом* — обеспечивает хранение прав доступа к ресурсам файловой системы и разграничение доступа пользователей к этим ресурсам.

При обращении пользователя к ресурсам компьютера (файлам, каталогам или устройствам) специальные модули перехватывают это обращение. Далее управление переходит к драйверам защитных подсистем, которые выполняют профильные действия, соответствующие цели обращения пользователя к ресурсу.

Информацию для выполнения действий драйверы защитных подсистем получают от ядра при инициализации подсистемы, при входе пользователя и в определенные моменты работы системы. Информация может быть получена драйверами как в процессе инициализации подсистем при загрузке компьютера, так и по запросу защитной подсистемы при обработке обращения пользователя к ресурсу. Загрузку необходимой информации через API защитных подсистем при инициализации и по запросу осуществляет служба ядра.

Модуль входа

Совместно с ОС Windows модуль входа в систему 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

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

Подсистема 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

Построение системы в сетевом режиме функционирования

Сетевой режим функционирования системы Secret Net предполагает использование компонентов, обеспечивающих возможность централизованного управления защищаемыми компьютерами. Для централизованного управления в системе должны быть установлены следующие программные средства:

• компонент "Secret Net 7 — Сервер безопасности". Для функционирования компонента требуется наличие системы управления базами данных (СУБД), реализуемой сервером СУБД Oracle или MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере;

• компонент "Secret Net 7" в сетевом режиме функционирования — на всех защищаемых компьютерах. На рабочих местах администраторов при установке компонента необходимо выбрать вариант с установкой средств централизованной настройки;

• 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.

Кроме того, если для централизованного управления параметрами групповых политик и/или параметрами доменных пользователей будут использоваться стандартные средства ОС Windows — дополнительно необходимо установить соответствующие компоненты ОС.

В сетевом режиме функционирования предоставляются возможности централизованного управления, мониторинга и получения локальных журналов для компьютеров, функционирующих под управлением ОС семейства Linux. Для этого на компьютерах должно быть установлено средство защиты информации Secret Net

LSP и выполнена настройка удаленного управления.

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.

В рамках леса доменов можно организовать функционирование нескольких серверов безопасности с подчинением по иерархическому принципу. При этом иерархия подчинения серверов не обязательно должна соответствовать структуре доменов в лесе. На рисунке 8 представлен пример использования нескольких серверов СБ1 — СБ4.

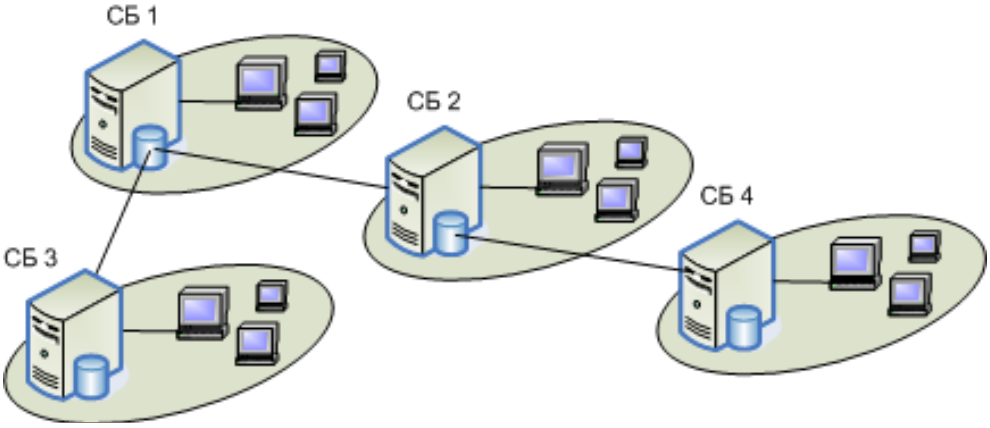

Рис.8. Пример использования нескольких серверов безопасности.

Каждый сервер контролирует работу своей группы защищаемых компьютеров и имеет свою базу данных. При этом некоторые операции доступны и в отношении объектов, относящихся к подчиненным серверам. Как видно из рисунка, серверы безопасности СБ2 и СБ3 являются подчиненными по отношению к СБ1, а СБ4 — подчиненным по отношению к СБ2.

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).
ТМ устройство сенсорной памяти Touch Memory.

Разработал:
доцент кафедры, к.п.н.

В. Мордовин

«____» _____ 201 года

Рецензировал:

«____» _____ 201 года