ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ЗАЩИТЫ ИНФОРМАЦИИ

Программно-аппаратный комплекс «Аккорд – 1.95»

1.1 Общие сведения

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «Аккорд – 1.95», далее комплекс «Аккорд», предназначен для применения на ПЭВМ типа IBM PC в целях защиты ПЭВМ и информационных ресурсов от НСД и обеспечения конфиденциальности информации, обрабатываемой и хранимой в ПЭВМ при многопользовательском режиме ее эксплуатации.

Комплекс разработан ОКБ САПР при участии фирмы «Инфокрипт» на основании лицензии Государственной технической комиссии при Президенте РФ (Гостехкомиссии России) от 02.06.95 N 56.

Комплекс «Аккорд» состоит из программно-аппаратных средств «Аккорд АМДЗ» и ПО разграничения доступа «Аккорд 1.95-00».

В настоящее время комплекс «Аккорд-1.95» выпускается в трех основных версиях в зависимости от модификации аппаратных средств (контроллеров):

версия 2.0 – контроллер «Аккорд – 4++»;

версия 3.0 – контроллер «Аккорд – 5»;

версия 4.0 – контроллер «Аккорд – 4.5»; «Аккорд – СБ/2».

Все модификации:

Могут использоваться на ПЭВМ с процессором 80386 и выше, объемом RAM 640 Кбайт и более.

Для установки необходим свободный слот:

ISA – для контроллеров «Аккорд – 4++», «Аккорд – 4.5»;

PCI – для контроллера «Аккорд – 5»; «Аккорд – СБ/2».

Используют для идентификации персональные ТМ-идентификаторы DS 199X с объемом памяти до 64 Кбит.

Используют для аутентификации пароль до 12 символов.

Блокируют загрузку с FDD, CD ROM, ZIP Drive.

Предусматривают регистрацию от 16 до 32 пользователей.

Имеют аппаратный датчик случайных чисел (ДСЧ).

Имеют возможность применения съемника, использующего внутреннее подключение к контроллеру (внутренний съемник).

Обеспечивают контроль целостности программ, данных и системных областей жестких дисков.

Имеют внутреннюю энергонезависимую память для хранения данных о зарегистрированных пользователях и журнала регистрации событий.

Допускают изменение встроенного ПО (технологический режим) без замены платы контроллера.

Обеспечивают режим доверенной загрузки ОС (выполнение процедур идентификации/аутентификации пользователя, контроль целостности аппаратной части ПЭВМ, системных файлов, программ и данных до загрузки ОС на аппаратном уровне).

Особенности этих модификаций приведены в таблице 1.

Таблица 1

Особенности различных типов контроллеров	«Аккорд-4++»	«Аккорд-4.5»	«Аккорд-5», «Аккорд СБ/2»
Тип используемой системной шины	ISA	ISA	PCI
Установка реле управления физическими линиями (5В, 300 Ма)	Не предусмотрена	Возможна установка 1-го или 2-х реле по заказу	Возможна установка 1-го или 2-х реле по заказу
Возможность перепрограммирования всех элементов без изменения аппаратной части	+	+	+
Установка таймера реального времени с собственным источником питания	Не предусмотрена	Возможна установка по заказу	Возможна установка по заказу
Установка датчика случайных чисел для криптографических применений	Не предусмотрена	Производится для всех контроллеров данного типа	Производится для всех контроллеров данного типа

Продолжение табл. 1

Особенности различных типов контроллеров	«Аккорд-4++»	«Аккорд-4.5»	«Аккорд-5», «Аккорд СБ/2»
Установка интерфейса RS 232 для считывателя smart-карт	Не предусмотрена	Не предусмотрена	Возможна установка по заказу

1.2 Технические и организационные сведения

Для установки комплекса «Аккорд» требуется следующий минимальный состав технических и программных средств:

- IBM PC AT совместимую ПЭВМ (с процессорами 80386 и старше);
- наличие на ПЭВМ HDD;
- наличие свободного слота на материнской плате ПЭВМ (ISA, PCI);
- операционная система MS DOS v.3.10 и выше.

Объем дискового пространства, необходимого для установки программных средств комплекса, составляет от 700 Кб до 1,2 Мб в зависимости от модификации программных средств комплекса.

Количество идентификаторов, используемых в комплексе «Аккорд», определяется заказчиком при поставке.

Комплекс «Аккорд» проверен на совместимость практически со всем доступным разработчику программно-аппаратным обеспечением ПЭВМ как зарубежного, так и отечественного производства. Совместимость обеспечивается правильной установкой и настройкой комплекса.

Для эффективного применения комплекса и поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов необходимы:

- физическая охрана ПЭВМ и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;
- наличие администратора службы безопасности информации (СБИ) – привилегированного пользователя, имеющего осо-

бый статус и абсолютные полномочия (супервизора). Администратор СБИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в ПЭВМ, эксплуатацию и контроль за правильным использованием ПЭВМ с внедренным комплексом, в том числе учет выданных ТМ-идентификаторов, осуществляет периодическое тестирование средств защиты комплекса.

- использование в ПЭВМ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ.

Применение комплекса «Аккорд» совместно с сертифицированными программными средствами криптографической защиты информации (СКЗИ) и/или программными средствами защиты информации от НСД (СЗИ НСД) позволяет значительно снизить нагрузку на организационные меры защиты информации, определенные условиями применения этих средств. При этом класс защищенности не снижается.

1.3 Особенности защитных функций комплекса

Комплекс «Аккорд» – это простой, но чрезвычайно эффективный комплекс технических средств, используя который можно надежно защитить информацию на компьютере без переделки ранее приобретенных программных средств.

Защитные функции комплекса реализуются применением:

1. Дисциплины защиты от НСД к ПЭВМ, включая идентификацию пользователя по уникальному ТМ-идентификатору и аутентификацию с учетом необходимой длины пароля и времени его жизни, ограничением времени доступа субъекта к компьютеру.

2. Процедур блокирования экрана и клавиатуры в случаях, в которых могут реализовываться угрозы информационной безопасности.

3. Дисциплины разграничения доступа к ресурсам АС (ПЭВМ), определяемой атрибутами доступа, которые устанавливаются администратором БИ в соответствие каждой паре «субъект доступа – объект доступа» при регистрации пользователей.

4. Дисциплины применения специальных процедур печати, управления стандартными процедурами печати, процедурами ввода/вывода на отчуждаемые носители информации.

5. Контроля целостности критичных с точки зрения информационной безопасности программ и данных (дисциплины защиты от несанкционированных модификаций).

6. Средств функционального замыкания информационных систем за счет использования средств защиты комплекса.

7. Других механизмов защиты в соответствии с требованиями нормативных документов по безопасности информации.

Комплекс «Аккорд» может применяться в произвольной и функционально замкнутой программной среде, обеспечивая при этом класс защищенности АС (ПЭВМ) 1В по классификации, надежно гарантируя при этом:

- защиту от несанкционированного доступа к АС (ПЭВМ) и ее ресурсам;
- разграничение доступа к ресурсам, в т.ч. к внешним устройствам, в соответствии с уровнем полномочий пользователей;
- защиту от несанкционированных модификаций программ и данных, внедрения разрушающих программных воздействий (РПВ);
- контроль целостности программ и данных;
- функциональное замыкание информационных систем с исключением возможности несанкционированного выхода в ОС, загрузки с FDD и несанкционированного прерывания контрольных процедур с клавиатуры.

Отметим, что в комплексе «Аккорд» используются и некоторые дополнительные механизмы защиты от НСД к ПЭВМ (АС). Так, в частности, для пользователя администратор БИ может установить:

- время жизни пароля и его минимальную длину, практически исключая тем самым возможность быстрого его подбора;
- временные ограничения использования ПЭВМ установкой интервала времени по дням недели (с дискретностью 30 мин), в котором разрешена работа для данного пользователя;
- параметры управления экраном – гашение экрана через заранее определенный интервал времени (в случае, если в течение указанного интервала действия оператором не выполнялись). Возможность продолжения работы предоставляется только после

проведения повторной идентификации по персональному ТМ-идентификатору пользователя;

- целесообразного с точки зрения критичности информационной безопасности объема конфиденциальной информации, выводимого на внешние устройства ПЭВМ;

- подачу соответствующих звуковых и визуальных сигналов при попытках несанкционированного доступа к ПЭВМ (АС) и ее ресурсам.

Предусмотрено подключение подсистемы криптографической защиты информации, которая позволяет пользователю зашифровать/расшифровать свои данные с использованием индивидуальных ключей, хранящихся в персональном ТМ-идентификаторе. Поставка криптографических систем защиты информации (в соответствии с действующим законодательством) и библиотеки программ для программирования работы с контроллером комплекса «Аккорд» оговаривается при заказе комплекса.

5.1.4 Построение системы защиты информации на основе комплекса

Построение системы защиты информации с использованием комплекса «Аккорд» и ее взаимодействие с программно-аппаратным обеспечением ПЭВМ показаны на рис. 5.1.

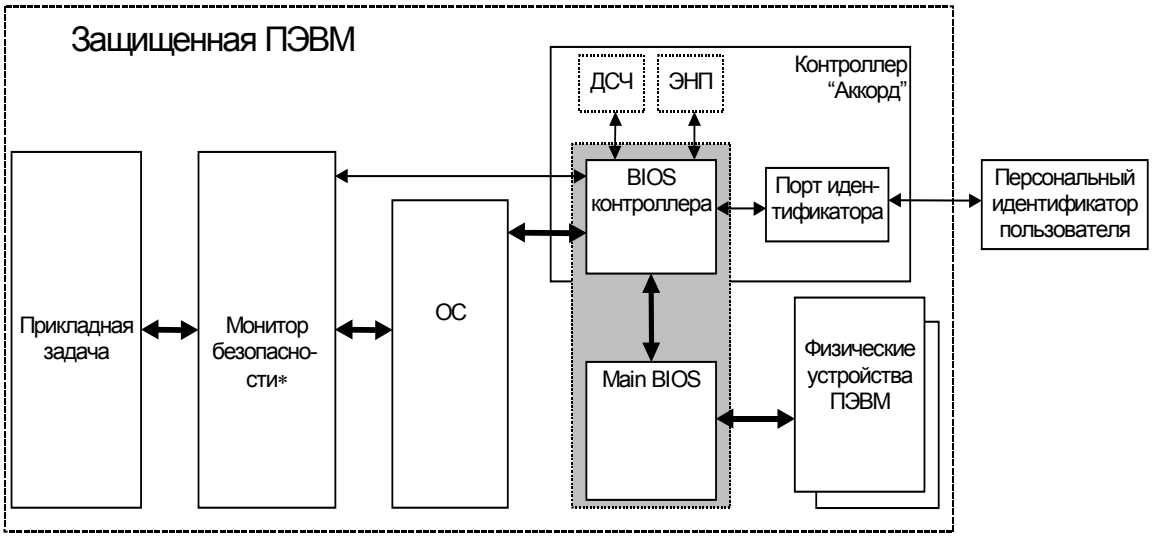

Рис. 5.1

Защита информации с использованием средств комплекса основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам ПЭВМ. При этом средства комплекса перехватывают соответствующие программные и/или аппаратные прерывания, в случае возникновения контролируемого события (запрос прерывания) анализируют запрос и в зависимости от соответствия полномочий субъекта доступа (его прикладной задачи), установленных администратором БИ ПРД, либо разрешают, либо запрещают обработку этих прерываний.

Комплекс «Аккорд» состоит из собственно средств защиты ПЭВМ от НСД и средств разграничения доступа к ее ресурсам, которые условно можно представить в виде четырех взаимодействующих между собой подсистем (рис. 5.2.) защиты информации.

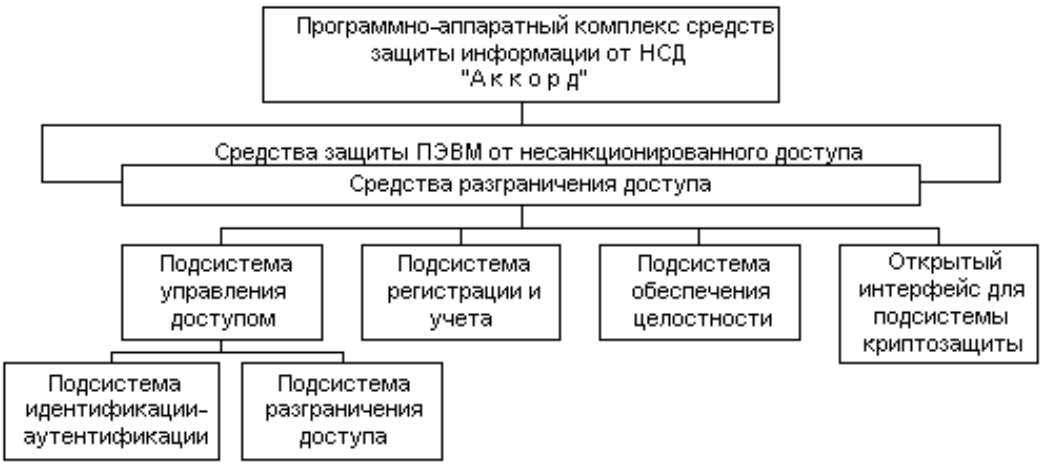

Рис. 5.2

5.1.4.1 Подсистема управления доступом

Предназначена для защиты ПЭВМ от посторонних пользователей, управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного в конкретной ПЭВМ ТМ-идентификатора). Защита от посторонних пользователей обеспечивается процедурами иден-

тификации (сравнение предъявленного ТМ-идентификатора с перечнем зарегистрированных на ПЭВМ) и аутентификации (подтверждение подлинности) с защитой от раскрытия пароля. Для идентификации (аутентификации) пользователей в комплексе «Аккорд» используются интеллектуальные персональные идентификаторы DS 199X («Touch memory» – «память касания»), отличающиеся высокой надежностью, уникальностью, наличием быстродействующей памяти, удобством пользования, приемлемыми массо-габаритными характеристиками и низкой ценой.

В комплексе «Аккорд» реализован принцип дискреционного управления доступом. Зарегистрированному пользователю устанавливаются права доступа по принципу регистрации «белого списка» разрешенных к запуску программ (задач), которые прописываются в ПРД. При запросе пользователя на доступ, обеспечивается однозначное трактование установленных ПРД, и, в зависимости от уровня полномочий пользователя, разрешается или запрещается запрошенный тип доступа.

5.1.4.2 Подсистема регистрации и учета

Предназначена для регистрации в системном журнале различных событий, происходящих в ПЭВМ. При регистрации событий в системном журнале регистрируются:

- дата и время события;
- пользователь, осуществляющий регистрируемое действие;
- действия пользователя (сведения о входе/выходе пользователя из системы, запусках программ, событиях НСД, изменении полномочий и др.).

Доступ к системному журналу возможен только администратору СБИ (супервизору).

В системный журнал заносятся сведения более чем о 200 событиях, а также осуществляется архивация занесенных данных.

5.1.4.3 Подсистема обеспечения целостности

Предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) программной среды, в том числе программных средств комплекса, обрабаты-

ваемой информации, обеспечивая при этом защиту ПЭВМ от внедрения программных закладок и вирусов. В комплексе «Аккорд» это реализуется:

- проверкой целостности назначенных для контроля системных файлов, в том числе КСЗИ НСД, пользовательских программ и данных;
- контролем обращения к операционной системе напрямую, в обход прерываний DOS;
- исключением возможности использования ПЭВМ без контроллера комплекса;
- механизмом создания замкнутой программной среды, запрещающей запуск привнесенных программ и исключающей несанкционированный выход в ОС.

При проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным (контрольным) значением, хранящимся в ТМ-идентификаторе пользователя. Эти данные заносятся при регистрации пользователя и могут изменяться в процессе эксплуатации ПЭВМ. В комплексе «Аккорд» используется сложный алгоритм расчета контрольных сумм (вычисление значения их хэш-функций), исключающий факт необнаружения модификации файла. Эталонное (контрольное) значение хэш-функции контрольной суммы хранится вне ПЭВМ, в ТМ-идентификаторе пользователя, и этим защищается от несанкционированной модификации. Защита от модификации программы расчета хэш-функций обеспечивается тем, что она хранится в микросхеме ПЗУ контроллера комплекса.

5.1.5 Состав комплекса

Комплекс «Аккорд» включает программные и аппаратные средства.

5.1.5.1 Аппаратные средства

Аппаратные средства содержат:

- одноплатный контроллер (ТУ РБ 28591037.001-95), устанавливаемый в свободный слот материнской платы ПЭВМ;

- контактное устройство-съемник информации (4012-003-11443195-97 93). Устанавливается обычно на передней панели ПЭВМ в отверстие, высверливаемое в заглушке на зарезервированном месте для дисковода, либо в другом подходящем месте (в зависимости от модификации съемника). Предусматривается установка внешнего съемника. При этом подключение осуществляется к задней планке контроллера посредством разъема RJ-11;

- интеллектуальный персональный идентификатор DS 199X («Touch memory» – «память касания») – ТМ-идентификатор. Представляет собой полупассивное микропроцессорное устройство, снабженное элементом питания, в виде «таблетки» диаметром 16 мм и толщиной 3–5 мм в удобной пластмассовой (металлической) оправке. Каждый ТМ-идентификатор обладает уникальным номером (48 бит), который формируется технологически и подделать который практически невозможно. Объем памяти, доступной для записи и чтения, составляет до 64 Кбит в зависимости от типа идентификатора. Срок хранения записанной информации, обеспечиваемый элементом питания, составляет не менее 10 лет.

Количество и тип ТМ-идентификаторов, модификации контроллера и контактного устройства оговаривается при поставке комплекса.

5.1.5.2 Программные средства

Программное обеспечение СЗИ «Аккорд 1.95-00»:

ACED32.EXE	Редактор прав доступа
ACRUN.EXE	Монитор безопасности
ACCORD.SYS	Драйвер п/с защиты ПЭВМ от НСД
TMDRV.EXE	Драйвер контроллера
ACSETUP.EXE	Установка подсистемы И/А
ACCORD.RES	Библиотека ресурсов
ACLOGPP.EXE	Препроцессор журнала
ACLOG.EXE	Работа с журналом

TMTEST.EXE	Диагностика идентификаторов
MEMSCAN.EXE	Анализ памяти для установки джамперов
CHECSUM.EXE	Вычисление контрольных сумм
ACNED.EXE	Редактор прав доступа в сети
ACCON.EXE	Консоль наблюдения
ACCIPX.EXE	Сетевой драйвер консоли
ACRIPX.EXE	Сетевой драйвер станции
ACSHEDNW.EXE	Диспетчер прав доступа (планировщик)

Программный интерфейс к контроллеру комплекса, включающий в себя объектные модули и модули заголовков для Borland Pascal v.7.0 и Borland C++ v.3.1, а также примеры использования интерфейса.

5.1.6 Принцип работы комплекса

Плата контроллера комплекса «Аккорд» устанавливается в свободный слот материнской платы ЭВМ, производится установка программного обеспечения на жесткий диск, настройка комплекса, в том числе установление прав разграничения доступа, и регистрация пользователей. При регистрации пользователя администратором СБИ определяются его права доступа: списки исполняемых программ и модулей, разрешенных к запуску данным пользователем, и список стартовых (исполняемых непосредственно после загрузки ОС) программ и др. С помощью утилиты ACED32.EXE в специальные файлы данных вносятся списки файлов, целостность которых будет проверяться при запуске ПЭВМ данным пользователем. Значение хэш-функции (контрольной суммы) этих файлов прописывается в память персонального ТМ-идентификатора. После регистрации пользователю выдается на руки персональный ТМ-идентификатор, о чем делается запись в журнал учета носителей информации. Особенностью и, несомненно, преимуществом комплекса «Аккорд» является проведение процедур идентификации, аутентификации и контроля целостности защищаемых файлов до загрузки операционной системы. Это обеспечивается при помощи ПЗУ, установ-

ленного на плате контроллера комплекса, которое получает управление во время так называемой процедуры ROM-SCAN. Суть данной процедуры в следующем. В процессе начального старта после проверки основного оборудования BIOS компьютера начинает поиск внешних ПЗУ в диапазоне от С 800:0000 до Е000:0000 с шагом в 2К. Признаком наличия ПЗУ является наличие слова АА55Н в первом слове проверяемого интервала. Если данный признак обнаружен, то в следующем байте содержится длина ПЗУ в страницах по 512 байт. Затем вычисляется контрольная сумма всего ПЗУ, и если она корректна, то будет произведен вызов процедуры, расположенной в ПЗУ со смещением. Такая процедура обычно используется для инициализации. В комплексе «Аккорд» в этой процедуре проводится идентификация и аутентификация пользователя, и при ошибке возврат из процедуры не происходит, т.е. загрузка выполняться не будет.

ПЗУ контроллера «Аккорд» использует прерывание int 13h (дисковый ввод/вывод). Если в ПЭВМ установлен контроллер диска, имеющий ПЗУ, которое участвует в процедуре ROM-SCAN (например, SCSI-контроллеры, контроллеры с аппаратной памятью и т.п.), то ПЗУ такого контроллера должно иметь более младший адрес, чем ПЗУ « Аккорда».

При установленном и инсталлированном комплексе «Аккорд» загрузка компьютера осуществляется в следующем порядке.

1. BIOS компьютера выполняет стандартную процедуру POST (проверку основного оборудования компьютера) и по ее завершении переходит к процедуре ROM-SCAN, во время которой управление перехватывает контроллер комплекса «Аккорд». На монитор выводится сообщение:

«Access system BIOS v.1.xx copyright OKB SAPR 1993.– 1995_ s/n.....»

2. Выводится окно с приглашением пользователю предъявить свой ТМ-идентификатор:

«Attach key, please...»

Это окно остается на мониторе до момента контакта ТМ-идентификатора пользователя и съемника информации.

3. Если идентификатор не зарегистрирован, то выводится сообщение:

«Access denied!»

и происходит возврат к п.2.

4. При легальном ТМ-идентификаторе выводится окно с приглашением пользователю ввести пароль для аутентификации:

«Password»

5. При неправильно введенном пароле выводится сообщение:

«Access denied!»

и происходит возврат к п.2.

6. При правильно введенном пароле выводится сообщение:

«Access granted!»

и продолжается процедура загрузки DOS и т.д.

Вся процедура идентификации и аутентификации занимает 7–10 секунд. Устойчивость ее зависит от длины пароля. Допускается установка пароля от 3 до 12 символов. При осуществлении контрольных процедур (идентификации и аутентификации пользователя, проверке целостности) драйвер ACCORD.SYS блокирует клавиатуру и загрузку ОС с диска А. При касании съемника информации осуществляется поиск предъявленного ТМ-

идентификатора в списке зарегистрированных на ПЭВМ идентификаторов. Обычно список хранится на диске С.

Если предъявленный ТМ-идентификатор обнаружен в списке, то производится контроль целостности защищаемых по перечню данного пользователя файлов. При проверке перечня файлов пользователя на целостность программой CHECKSUM.EXE вычисляется хэш-функция контрольной суммы этих файлов и сравнивается с эталонным (контрольным) значением, считываемым из предъявленного персонального ТМ-идентификатора. Для проведения процедуры аутентификации предусмотрен режим ввода пароля в скрытом виде – в виде символов <*>. Этим предотвращается возможность раскрытия индивидуального пароля и использования утраченного (похищенного) ТМ-идентификатора. При положительном результате указанных выше контрольных процедур появляется сообщение «Access granted!» («Доступ разрешен») на зеленом фоне и производится загрузка DOS. Если предъявленный пользователем идентификатор не зарегистрирован в списке (сообщение «Неизвестный идентификатор») или нарушена целостность защищаемых файлов (сообщение «Нарушение целостности»), загрузка DOS не производится. Для продолжения работы потребуется вмешательство администратора СБИ. Таким образом, контрольные процедуры (идентификация, аутентификация, проверка целостности системных файлов ОС) осуществляются до загрузки ОС, при этом обеспечивается защита от РПВ. В любом другом случае, т.е. при неподтверждении прав пользователя на работу с данной ПЭВМ, загрузка DOS не выполняется. При выполнении модифицированных администратором СБИ в процессе установки комплекса файлов CONFIG.SYS и AUTOEXEC.BAT производится блокировка клавиатуры, загрузка модуля ACRUN.EXE, осуществляющего контроль за использованием пользователем только разрешенных ему ресурсов и запускающего (на основании проведенной идентификации/ аутентификации) стартовую пользовательскую задачу. В процессе работы пользователя программа ACRUN.EXE препятствует любым видам НСД к файлам CONFIG.SYS и AUTOEXEC.BAT.

Механизм контроля целостности реализуется процедурой сравнения двух векторов для одного массива данных: эталонного (контрольного), выработанного заранее на этапе регистрации

пользователей, и текущего, выработанного непосредственно перед проверкой. Эталонный (контрольный) вектор вырабатывается на основе хэш-функций (контрольной суммы) защищаемых файлов и хранится в идентификаторе. В случае санкционированной модификации защищенных файлов осуществляется процедура перезаписи в идентификатор нового значения хэш-функции (контрольной суммы) модифицированных файлов, для чего на экране выдается сообщение «Прислоните ТМ-идентификатор» с последующим подтверждением успешной (неуспешной) перезаписи значения хэш-функции в персональный идентификатор пользователя. В процессе функционирования комплекса резидентная часть «монитора безопасности» проверяет файлы всех загруженных из файла CONFYG.SYS драйверов и обеспечивает оперативный контроль целостности исполняемых файлов перед передачей им управления. Тем самым обеспечивается защита от программных вирусов и закладок. В случае положительного исхода проверки управление передается ОС для загрузки файла на исполнение. При отрицательном исходе проверки запуск программы не происходит.

Кроме того, «монитор безопасности» ограничивает доступ к файлам ПО комплекса, которые расположены в каталоге C:\ACCORD, запрещая пользователю их переименование, уничтожение, изменение (запись и редактирование). Таким же образом защищены и файлы AUTOEXEC.BAT и CONFIG.SYS (поскольку удаление из них вызовов программной части комплекса может привести к возможности НСД). Для защиты от извлечения платы контроллера комплекса используется специальный механизм, обеспечивающий выполнение нормальной загрузки DOS только при наличии платы. При отсутствии платы загрузка DOS не осуществляется.

Работа программы с журналами регистрации приведена в приложении 3.

5.2 Программно-аппаратный комплекс Secret Net NT 4.0

5.2.1 Функциональные возможности системы

Автономный вариант системы защиты информации Secret Net NT 4.0 предназначен для защиты ресурсов рабочей станции локальной сети или неподключенного к сети компьютера и разработан научно-инженерным предприятием «ИНФОРМЗАЩИТА».

Система Secret Net NT 4.0 дополняет стандартные защитные механизмы ОС Windows NT функциями, обеспечивающими:

- идентификацию пользователей при помощи специальных аппаратных средств (Touch Memory, Smart Card, Smarty);
- дополнительно к избирательному (дискреционному) управлению доступом, реализованному в ОС Windows NT, полномочное (мандатное) управление доступом пользователей к конфиденциальной информации на локальных и подключенных сетевых дисках;
- оперативный контроль работы пользователей компьютера путем регистрации событий, связанных с безопасностью ИС, удобные средства просмотра и представления зарегистрированной информации;
- контроль целостности программ, используемых пользователями и операционной системой;
- возможность создания для любого пользователя замкнутой программной среды (списка разрешенных для запуска программ);
- простоту управления объектами благодаря использованию механизма шаблонов настроек.

5.2.2 Общая архитектура

Система Secret Net NT включает в себя следующие компоненты и подсистемы:

- ядро системы защиты (1);
- подсистема управления (4);
- подсистема криптографической защиты информации (5);
- база данных системы защиты (6);

- подсистема избирательного управления доступом (9);
- подсистема разграничения доступа к дискам (10);
- подсистема разграничения полномочного доступа (11);
- подсистема замкнутой программной среды (12);
- подсистема контроля целостности (14);
- подсистема контроля входа (16).

На рис. 1 приведена обобщенная структура автономного варианта системы защиты Secret Net NT, представлены основные элементы и взаимосвязи между ними.

5.2.3 Основные компоненты

Ядро системы защиты (1) представляет собой программу, которая автоматически запускается на защищенном компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Ядро системы осуществляет управление подсистемами и компонентами системы защиты и обеспечивает их взаимодействие.

В процессе работы системы защиты ядро выполняет следующие функции:

- обеспечивает обмен данными между компонентами системы и обработку команд, поступающих от этих компонент;
- обеспечивает доступ других компонент системы к информации, хранящейся в базе данных системы защиты;
- осуществляет сбор сведений о состоянии компьютера;
- контролирует доступ пользователя к ресурсам компьютера;
- обрабатывает информацию, поступающую от компонент системы защиты, о событиях, происходящих на компьютере и связанных с безопасностью системы, и осуществляет их регистрацию в журнале безопасности ОС Windows NT.

Подсистема регистрации (3) является одним из элементов ядра системы и предназначена для управления регистрацией в журнале безопасности Windows NT (8) событий, связанных с работой ОС и Secret Net. Эта информация поступает от отдельных подсистем системы защиты, которые следят за происходящими в информационной среде событиями. Регистрация событий осуще-

ствляется системными средствами (ОС Windows NT) или средствами системы защиты Secret Net NT. Перечень регистрируемых событий устанавливается администратором с помощью подсистемы управления (4). Для просмотра журнала используется специальная программа подсистемы управления, обладающая развитыми средствами работы с журналами регистрации.

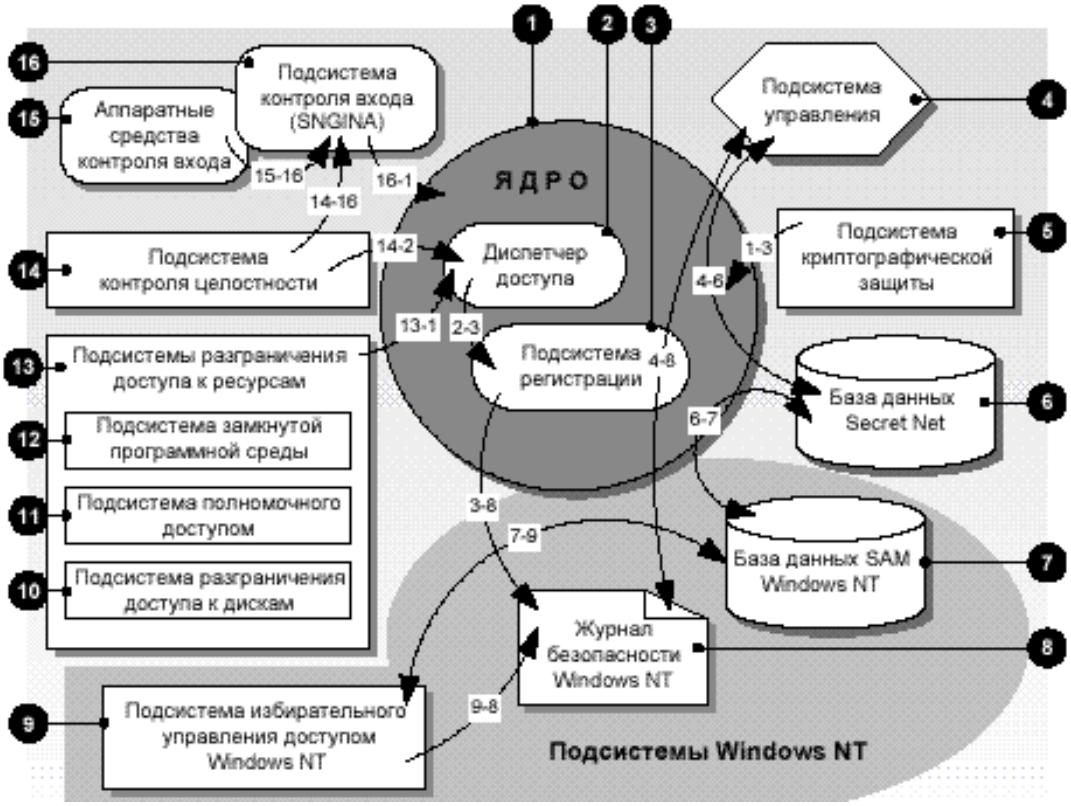

Рис. 1 – Архитектура автономного варианта системы Secret Net NT

Подсистема управления (4) располагает средствами для настройки защитных механизмов через управление общими параметрами работы компьютера, свойств пользователей и групп пользователей. В частности она обеспечивает:

- отображение и управление состоянием защищаемого компьютера;
- управление пользователями, настройками компьютера и сохранение относящихся к ним данных в БД системы защиты (6);
- получение информации из БД системы защиты;
- обработку и представление информации из журнала безопасности ОС Windows NT (8).

В состав подсистемы управления входит программа, предназначенная для просмотра журнала безопасности и подготовки отчетов. С ее помощью можно выполнить просмотр, отбор, сортировку, поиск записей, печать, экспорт журнала в другие форматы.

База данных Secret Net (6) предназначена для хранения сведений, необходимых для работы защищенного компьютера. БД Secret Net размещается в реестре ОС Windows NT и содержит информацию об общих настройках системы защиты, свойствах пользователей и групп пользователей.

Доступ подсистем и компонент системы защиты к данным, хранящимся в БД Secret Net, обеспечивается ядром системы защиты (1).

Первоначальное заполнение БД выполняется при установке Secret Net. Для этого используются данные, содержащиеся в БД безопасности Windows NT (политика безопасности, состав пользователей и групп пользователей и т.д.), и данные, устанавливаемые по умолчанию для Secret Net (значения общих параметров, некоторые свойства пользователей, набор шаблонов и т.д.).

Синхронизацию данных в БД безопасности Windows NT и БД Secret Net.обеспечивает ядро системы защиты (1). В дальнейшем информация, содержащаяся в БД, создается и модифицируется подсистемой управления (4) и другими подсистемами.

Подсистема избирательного управления доступом (9) обеспечивает разграничение доступа пользователей к ресурсам файловой системы, аппаратным ресурсам и ресурсам операционной системы компьютера.

Для управления доступом к ресурсам файловой системы, системному реестру и системным средствам управления компьютером используются стандартные средства ОС Windows NT, а непосредственное управление осуществляется с использованием интерфейса Secret Net NT. Для управления доступом к остальным ресурсам (дискам и портам) используются средства Secret Net NT.

Подсистема полномочного управления доступом (11) обеспечивает разграничение доступа пользователей к конфиденциальной информации, хранящейся в файлах на локальных и сетевых дисках. Доступ осуществляется в соответствии с категорией конфиденциальности, присвоенной информации, и уровнем допуска пользователя к конфиденциальной информации.

Подсистема полномочного управления доступом включает в себя драйвер полномочного управления доступом и компоненту управления допуском к ресурсам.

Компонента управления конфиденциальностью ресурсов включается в программу «Проводник» (Explorer). Из программы «Проводник» и осуществляется управление категориями конфиденциальности, которые присваиваются файлам, каталогам и дискам компьютера. Диски обязательно должны быть размечены для работы с файловой системой NTFS.

Драйвер полномочного управления доступом контролирует доступ пользователей к конфиденциальным ресурсам. Когда пользователь (или программа, запущенная пользователем) осуществляет попытку выполнить какую-либо операцию над конфиденциальным ресурсом, драйвер определяет категорию конфиденциальности ресурса и передает ее диспетчеру доступа (2), входящему в состав ядра системы защиты. Диспетчер доступа сопоставляет категорию конфиденциальности ресурса и уровень допуска данного пользователя к конфиденциальной информации. Также он проверяет, не противоречат ли действия пользователя с ресурсом другим настройкам системы (например, условиям копирования через буфер обмена). Если уровень допуска или настройки системы не позволяют выполнить операцию – диспетчер доступа передает драйверу запрещающую команду, и операция блокируется. При этом подсистема регистрации (3) ядра системы фиксирует в журнале попытку несанкционированного доступа.

Подсистема замкнутой программной среды (11) позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска.

Драйвер замкнутой программной среды контролирует запуск пользователем программ. Когда пользователь (программа,

запущенная пользователем) осуществляет попытку запуска какой-либо программы, драйвер передает диспетчеру доступа (2), входящему в состав ядра системы защиты, сведения о запускаемой программе. Диспетчер доступа проверяет, включена ли эта программа в персональный список программ, разрешенных для запуска. Если программа содержится в списке, диспетчер доступа передает драйверу разрешающую команду. Если пользователю запрещено запускать данную программу, диспетчер доступа передает драйверу запрещающую команду, и запуск программы блокируется. В этом случае подсистема регистрации (3) фиксирует в журнале безопасности попытку несанкционированного доступа.

Подсистема контроля входа (16) обеспечивает идентификацию и аутентификацию пользователя при его входе в систему. Подсистема включает в себя модуль идентификации пользователя, а также может содержать средства аппаратной поддержки, например, Secret Net TM Card или электронный замок «Соболь», если они установлены на компьютере, и программу-драйвер, с помощью которой осуществляется управление аппаратными средствами.

Подсистема контроля входа запрашивает и получает информацию о входящем в систему пользователе (имя, пароль, персональный идентификатор, личный ключ пользователя). Затем сравнивает полученную информацию с информацией, хранящейся в БД системы защиты. Предоставление информации из БД обеспечивает ядро системы защиты. Если в БД отсутствует информация о пользователе, процедура загрузки системы прекращается.

Для целей идентификации и аутентификации могут использоваться аппаратные средства. Для управления ими необходимы специальные программы-драйверы, которые обеспечивают обмен информацией между устройствами аппаратной поддержки и модулями системы защиты. Драйверы входят в комплект поставки и устанавливаются на компьютер вместе с системой Secret Net NT.

При загрузке компьютера подсистема контроля целостности (14) проверяет целостность системных файлов. Если целостность файлов не нарушена, подсистема контроля целостности передает

управление подсистеме опознавания пользователя. В случае нарушения целостности файлов загрузка системы может быть запрещена.

Подсистема контроля целостности (14) осуществляет слежение за неизменностью контролируемых объектов (файлов, ключей системного реестра и т.д.) с целью защиты их от модификации. Для этого определяется перечень контролируемых объектов. Для каждого из входящих в него объектов рассчитываются эталонные контрольные суммы. Вычисления проводятся с использованием хэш-функций (в соответствии с ГОСТ Р 34-10) или по оригинальному (быстрому) алгоритму собственной разработки. Эталонные контрольные суммы проверяемых объектов и информация об их размещении хранятся в пакетах контроля целостности.

Целостность объектов контролируется в соответствии с установленным расписанием. Подсистема контроля входа (16) передает подсистеме контроля целостности **Secret Net NT 4.0.** перечень контролируемых объектов и порядок их контроля при запуске компьютера.

Ядро системы (1) передает подсистеме контроля целостности расписание контроля, составленное администратором с помощью подсистемы управления (4). В соответствии с расписанием контроля, вычисляются контрольные суммы проверяемых объектов и сравниваются с ранее вычисленными их эталонными значениями.

Если выявляется нарушение целостности объектов, подсистема контроля целостности сообщает об этом диспетчеру доступа (2).

5.2.4 Защитные механизмы Secret Net NT 4.0

Система Secret Net NT дополняет операционную систему Windows NT рядом защитных средств, которые можно отнести к следующим группам:

5.2.4.1 Средства защиты от несанкционированного входа в систему:

- механизм идентификации и аутентификации пользователей (в том числе с помощью аппаратных средств защиты);
- функция временной блокировки компьютера на время паузы в работе для защиты компьютера от использования посторонним лицом;
- функция программной защиты от загрузки ОС с гибкого диска;
- аппаратные средства защиты от загрузки ОС с гибкого диска.

5.2.4.2 Средства управления доступом и защиты ресурсов:

- разграничение доступа пользователей к ресурсам компьютера с использованием механизмов избирательного и полномочного управления доступом;
- создание для любого пользователя замкнутой программной среды (списка разрешенных для запуска программ);
- средства криптографической защиты данных: шифрование информации, хранящейся в файлах на сетевых и локальных дисках; вычисление и проверка электронной цифровой подписи (ЭЦП).

5.2.4.3 Средства регистрации и оперативного контроля:

- политика регистрации, ведение журнала регистрации событий, имеющих отношение к безопасности системы, работа с журналами, управление временем хранения и удалением записей;
- контроль целостности файлов, управление расписанием контроля и выбор реакции на нарушение целостности;
- контроль аппаратной конфигурации компьютера.

Отличительной особенностью системы Secret Net NT является возможность гибкого управления набором защитных средств системы. Пользователь, имеющий привилегии на администрирование системы, может активизировать различные комбинации защитных механизмов системы, выбирая из них только необходимые и устанавливая соответствующие режимы их работы.

5.2.5 Механизмы контроля входа в систему

Защита от несанкционированного входа предназначена для предотвращения доступа посторонних лиц к защищенному компьютеру. К этой группе средств, как уже говорилось, могут быть отнесены:

- программные и аппаратные средства идентификации и аутентификации;
- функция временной блокировки компьютера;
- аппаратные средства защиты от загрузки ОС с гибкого диска.

5.2.6 Механизм идентификации и аутентификации пользователей

Идентификация и аутентификация пользователей выполняется при каждом входе пользователя в систему. При загрузке компьютера система Secret Net NT запрашивает у пользователя его идентификатор и пароль. Затем проверяется, был ли зарегистрирован в системе пользователь с таким именем и правильно ли указан его пароль. В качестве идентификаторов могут использоваться: уникальные имена и уникальные номера аппаратных устройств идентификации (персональных идентификаторов).

В Secret Net NT поддерживается работа с паролями длиной до 16 символов. Если пароль указан неверно, подается звуковой сигнал и в журнале безопасности регистрируется попытка несанкционированного доступа к компьютеру. При определенном числе неверных попыток ввода пароля происходит блокировка компьютера.

Идентификаторы пользователей (имена и номера аппаратных идентификаторов) хранятся в базе данных системы защиты в открытом виде, а пароли пользователей – в кодированном виде.

5.2.7 Аппаратные средства защиты от несанкционированного входа

Средства аппаратной поддержки в системах защиты предназначены для:

- запрета загрузки ОС со съемных носителей (гибких и компакт-дисков);

- идентификации пользователей системы защиты до загрузки ОС;
- поддержки различных аппаратных идентификаторов (например, Touch Memory), заменяющих ввод идентифицирующей информации с клавиатуры.

Работу системы защиты с аппаратными средствами обеспечивают специальные программы-драйверы, управляющие обменом информацией между устройством и модулями системы защиты.

В системе Secret Net NT предусмотрено несколько режимов идентификации и аутентификации с использованием аппаратных средств. Это дает возможность проводить их внедрение поэтапно. При «мягком» режиме работы любой пользователь может войти в систему либо предъявив персональный идентификатор, либо указав свое имя. При «жестком» режиме вход в систему любого пользователя разрешен только при предъявлении персонального идентификатора.

5.2.8 Функция временной блокировки компьютера

Функция временной блокировки компьютера предназначена для предотвращения использования компьютера посторонними лицами. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора (хранителем экрана). Включить режим временной блокировки компьютера может сам пользователь, нажав определенную, заданную им, комбинацию клавиш.

Компьютер может быть заблокирован и автоматически после некоторого периода простоя. Длительность этого интервала устанавливается настройкой соответствующих параметров. Вывести компьютер из режима блокировки можно, только если вновь указать пароль или предъявить персональный идентификатор.

5.2.9 Механизмы управления доступом и защиты ресурсов

Система Secret Net NT включает в свой состав несколько механизмов управления доступом пользователей к ресурсам компьютера:

- механизм избирательного управления доступом;
- механизм полномочного управления доступом;

- механизм замкнутой программной среды.

Все ресурсы компьютера в системе Secret Net NT делятся на три типа:

Ресурсы файловой системы – локальные логические диски и размещающиеся на них каталоги и файлы.

Аппаратные ресурсы – локальные и сетевые принтеры, коммуникационные порты, физические диски, дисководы, приводы CD-ROM.

Ресурсы операционной системы – системные файлы, ключи системного реестра, системное время, диалоги настройки параметров системы.

Механизмы полномочного управления доступом и механизм замкнутой программной среды применяются только к ресурсам файловой системы.

5.2.10 Механизм избирательного управления доступом

Управление избирательным доступом к локальным ресурсам компьютера осуществляется на основании предоставления пользователям компьютера прав и привилегий.

В Secret Net NT для управления доступом к ресурсам файловой системы, системному реестру и системным средствам управления компьютером используются стандартные механизмы ОС Windows NT.

Примечание. Подробные сведения о механизме избирательного управления доступом в ОС Windows NT можно найти в документации к ОС. Для управления доступом к дискам и портам используются собственные механизмы системы Secret Net NT.

5.2.11 Механизм полномочного управления доступом

Система Secret Net NT включает в свой состав средства, позволяющие организовать полномочное (мандатное) управление доступом пользователей к конфиденциальной информации. Полномочное управление доступом осуществляется только по отношению к каталогам и распространяется на все файлы и подкаталоги, находящиеся в них. При организации полномочного управ-

ления доступом для каждого пользователя компьютера устанавливается некоторый уровень допуска к конфиденциальной информации, определяющий его права на доступ к конфиденциальным данным. Всем файлам и каталогам, находящимся на локальных дисках и подключенных сетевых дисках компьютера, назначается категория конфиденциальности. Используются три категории конфиденциальности информации: «Нет» (для общедоступной информации), «Конфиденциально», «Строго конфиденциально».

Доступ к конфиденциальным каталогам и находящимся в них файлам осуществляется следующим образом. Когда пользователь (программа, запущенная пользователем) осуществляет попытку доступа к конфиденциальному каталогу или находящемуся в нем файлу, диспетчер доступа Secret Net NT определяет категорию конфиденциальности данного ресурса. Затем категория конфиденциальности ресурса сопоставляется с уровнем допуска пользователя к конфиденциальной информации. Если текущий пользователь не превышает свой уровень допуска, система защиты санкционирует доступ к ресурсу. Иначе система защиты блокирует доступ к ресурсу.

При работе системы Secret Net NT в режиме полномочного управления доступом контролируются потоки конфиденциальной информации. Это позволяет, например, предотвратить копирование конфиденциальных документов в неконфиденциальные области дисков и запретить свободный доступ к принтерам и коммуникационному оборудованию. Печать конфиденциальных документов в этом случае осуществляется только стандартными средствами Secret Net и фиксируется в системном журнале.

5.2.12 Механизм замкнутой программной среды

Механизм замкнутой программной среды позволяет без использования системы атрибутов ограничить доступ пользователей к исполняемым файлам только теми программами, которые действительно необходимы ему для выполнения своих служебных обязанностей.

Режим замкнутой программной среды может быть активизирован избирательно для тех или иных пользователей. Преду-

смотрена возможность двух режимов работы этого механизма – «жесткого» и «мягкого». При «мягком» режиме пользователю разрешается запускать программы, не внесенные в список разрешенных для запуска, но при этом в системном журнале регистрируются соответствующие события несанкционированного доступа (НСД). При «жестком» режиме запуск любой программы, не внесенной в список разрешенных для запуска программ, будет блокироваться, а попытка запуска будет регистрироваться как событие НСД.

Примечание. В Secret Net NT средства защиты могут работать в двух режимах: «жестком» и «мягком». «Жесткий» режим является основным режимом работы системы защиты. Использование «мягкого» (технологического) режима облегчает настройку системы защиты при вводе ее в эксплуатацию. Анализируя случаи НСД, зарегистрированные при работе в этом режиме, администратор безопасности может, не ограничивая потребности пользователя в ресурсах, выявить и конкретизировать их.

Перечень программ, разрешенных для запуска, определяется индивидуально для каждого пользователя. Список может быть сформирован автоматически на основании сведений об используемых программах из системного журнала (в условиях «мягкого» режима работы) и отредактирован средствами специального редактора.

Сформированные списки разрешенных для запуска программ хранятся в файлах в подкаталоге UEL каталога, в который была установлена система Secret Net. Файлы имеют расширение .uel и имя, совпадающее с регистрационным номером пользователя в системе. Uel-файл – это обычный текстовый файл, содержащий в каждой строке полный путь к файлу программы, запуск которой разрешен.

5.2.13 Механизмы контроля и регистрации

Система Secret Net NT включает в свой состав следующие средства контроля:

- механизм регистрации событий;
- механизм контроля целостности.

5.2.14 Механизм регистрации событий

В процессе работы системы Secret Net NT события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журнале безопасности Windows NT. Относительно каждого события фиксируется следующая информация:

- дата и время, определяющие момент наступления события;
- идентификатор пользователя, действия которого привели к появлению события;
- краткая характеристика события;
- имя программы, работа которой привела к появлению события;
- ресурс, при работе с которым произошло событие.

В общей сложности в системный журнал заносятся сведения более чем о ста видах событий.

Механизм регистрации событий обладает гибкими возможностями управления. Для каждого пользователя можно определить индивидуальный режим регистрации. От общего объема регистрируемых событий зависит размер системного журнала и, соответственно, время записи и последующего анализа событий.

Для системного журнала может быть установлен предельный срок хранения регистрационных записей, по истечении которого устаревшие записи будут автоматически удаляться из журнала. Право на настройку режимов регистрации событий предоставляется пользователю посредством соответствующих привилегий на администрирование системы.

5.2.15 Механизм контроля целостности

Контроль целостности предназначен для слежения за изменениями характеристик выбранных объектов информационной среды. Объектами контроля могут быть: секторы дисков, файлы, каталоги, элементы реестра, ветви и настройки сервисов.

Каждый тип объектов имеет свой набор контролируемых данных. Так, например, файлы могут контролироваться на целостность: содержимого, прав доступа, атрибутов и существования.

Кроме того, для каждого из типов объектов могут использоваться различные алгоритмы контроля целостности.

В системе предусмотрена гибкая возможность выбора времени контроля. В частности, контроль может быть выполнен при загрузке ОС (средствами электронного замка «Соболь»), при входе или выходе пользователя из системы по заранее составленному расписанию. Кроме того, может быть проведен и немедленный контроль.

При обнаружении несоответствия предусмотрены следующие варианты реакции на возникающие ситуации подсистемы контроля целостности:

- регистрация изменений в системном журнале;
- оповещение администратора безопасности о произошедших изменениях;
- блокировка компьютера;
- отклонение или принятие изменений.

Для каждого типа контролируемых объектов на рабочей станции хранятся список имен объектов и задания для контроля тех или иных характеристик указанных объектов. Эта информация размещается в базе данных подсистемы контроля целостности, которая реализована в виде набора файлов определенного формата, расположенных в отдельном каталоге. База данных содержит всю необходимую информацию для функционирования подсистемы. Задание на контроль содержит необходимую информацию об эталонном состоянии объекта, порядке контроля характеристик и действий, которые надо выполнить при обнаружении изменений. Результаты контроля и обработки запросов фиксируются в системном журнале.

Подсистема контроля целостности взаимодействует с другими подсистемами через ядро системы защиты. Для просмотра и редактирования списков контроля целостности, режимов контроля и номенклатуры контролируемых объектов используется подсистема управления (4). Кроме того, подсистема контроля целостности самостоятельно выполняет контроль объектов и взаимодействует для выполнения различных действий со следующими подсистемами Secret Net:

- подсистемой контроля входа (16) – для оповещения о входе или выходе пользователя из системы;

- подсистемой аппаратной поддержки (15) – для получения доступа к аппаратным средствам контроля;
- подсистемой регистрации (3) – для записи сообщений в системный журнал;
- подсистемой криптографической защиты (5) – для выполнения криптографических операций при контроле целостности.

Подсистема контроля целостности используется в нескольких типичных случаях:

- для контроля в автоматическом режиме целостности объектов по установленному расписанию;
- для выполнения внеплановых проверок по инициативе администратора;
- для обработки запросов от программы управления с целью просмотра и изменения характеристик контролируемых объектов.

5.2.16 Контроль аппаратной конфигурации компьютера

Контроль аппаратной конфигурации компьютера предназначен для своевременного обнаружения изменений конфигурации и выбора наиболее целесообразного способа реагирования на эти изменения. Изменения аппаратной конфигурации компьютера могут быть вызваны выходом из строя, добавлением или заменой отдельных устройств.

Для эффективного контроля конфигурации используется широкий набор контролируемых параметров, с каждым из которых связаны правила обнаружения изменений и действия, выполняемые в ответ на эти изменения.

Сведения об аппаратной конфигурации компьютера хранятся в БД системы защиты. Первоначальные («эталонные») данные о конфигурации поступают от программы установки. Каждый раз при загрузке компьютера, а также при повторном входе пользователя система получает сведения об актуальной аппаратной конфигурации и сравнивает ее с эталонной.

Контроль конфигурации программных и аппаратных средств производится ядром системы Secret Net. По результатам контроля ядро принимает решение о необходимости блокировки компьютера. Решение принимается после входа пользователя и

зависит от настроек пользователя. Значение настроек пользователя определяет администратор безопасности.

Если было выполнено запланированное изменение конфигурации компьютера, то пользователь, обладающий административными привилегиями, может при помощи подсистемы управления обновить эталонные сведения о конфигурации.

5.2.17 Средства аппаратной поддержки Secret Net

В качестве средств аппаратной поддержки в Secret Net могут быть использованы следующие устройства:

Secret Net ROM BIOS – микросхема с расширением BIOS, устанавливается на сетевой карте компьютера в гнездо для микросхемы удаленной загрузки. Обеспечивает идентификацию с помощью электронных идентификаторов Touch Memory, считыватели которых подключены к COM -порту.

Secret Net Touch Memory Card – плата с разъемом для подключения считывателя Touch Memory или считывателя бесконтактных радиокарт Proximity, устанавливаемая внутри компьютера в разъем ISA. Обеспечивает идентификацию пользователей по электронным идентификаторам Touch Memory или картам Proximity.

Контроллер «Соболь» – плата с разъемом для подключения считывателя Touch Memory, аппаратным датчиком случайных чисел, 2-мя (4-мя) каналами физической блокировки устройств и внутренней энергонезависимой памятью. Устанавливается внутри компьютера в разъем ISA или PCI. Является основой системы Электронный замок «Соболь». В системе Secret Net может быть использован для идентификации пользователей по электронным идентификаторам Touch Memory, а также для генерации криптографических ключей.

Считыватель бесконтактных радиокарт Proximity – устройство, подключаемое к разъему Secret Net Touch Memory Card и устанавливаемое внутри корпуса компьютера. В системе Secret Net считыватель используется для идентификации пользователей по картам Proximity.