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 4: Информационные системы управления промышленным производством и основы защиты информации в САПР ТПП

Лекция № 10. Программно-технические средства защиты информации САПР ТПП

(2 часа)

Доцент кафедры, к.п.н.,

Мордовин В.Н.

2021 г.

СПб ГУТ)))

Учебные вопросы

1. Основные понятия.

2. Виды угроз безопасности в САПР.

3. Методы и средства защиты информации.

4. Аппаратно-программный модуль доверенной загрузки (АПМДЗ).

4.1. Назначение изделия.

4.2. Состав изделия.

4.3. Технические характеристики и устройство АПМДЗ.

4.4. Основные принципы функционирования АПМДЗ.

5. Система Secret Net.

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

5.2. Архитектура и средства управления.

5.3. Сетевая структура системы Secret Net.

Литература

1. СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (СТР-К) . М. 2001.

2. Баранов В.М. и др. Организация защиты информации. Учебное пособие. СПб, ВКА им.А.Ф.Можайского. 2015.

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

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

ВВЕДЕНИЕ

Различные субъекты по отношению к определенной информации могут выступать *в качестве* (возможно одновременно):

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается информация;
- владельцев систем сбора и обработки информации и участников процессов обработки и передачи информации и т.д.

Для успешного осуществления деятельности по управлению объектами некоторой предметной области субъекты информационных отношений *могут быть заинтересованы* в обеспечении:

- *своевременного доступа* к необходимой информации;
- *конфиденциальности* (сохранения в тайне) определенной части информации;
- *достоверности* (полноты, точности, адекватности, целостности) информации;
- *защиты от* навязывания ложной (недостоверной, искаженной) информации, т.е. от *дезинформации*;
- *защиты части информации от незаконного ее тиражирования* (защита авторских прав, прав собственника информации и т.п.);
- *разграничения законных прав* (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- *контроля и управления* процессами обработки и передачи информации.

Свойства информации и систем ее обработки:

- ***доступность*** информации, т.е. свойство системы в которой циркулирует информация, *характеризующаяся способностью обеспечивать своевременный беспрепятственный доступ субъектов* к интересующим их данным и готовностью соответствующих автоматизированных служб к выполнению поступающих от субъектов запросов;
- ***целостность*** информации, т.е. свойство информации, заключающееся в ее *существовании в неискаженном виде;*
- ***конфиденциальность*** информации - субъективно определяемая характеристика информации, указывающая на необходимость введения *ограничений на круг субъектов*, которые *имеют доступ к данной информации*.

1. Основные понятия

- ***Защита информации*** — это средства обеспечения безопасности информации.
- ***Безопасность информации*** — защита информации от утечки, модификации и утраты. *Сфера безопасности информации* — не защита информации, а *защита прав собственности* на нее и интересов субъектов информационных отношений.
- ***Утечка информации*** - ознакомление *постороннего лица* с содержанием секретной информации.
- ***Модификация информации*** — *несанкционированное изменение информации*, корректное по форме и содержанию, но *другое по смыслу*.
- ***Утрата информации*** — физическое *уничтожение* информации.
- ***Цель защиты информации*** — *противодействие угрозам* безопасности информации.

1. Основные понятия

- ***Угроза безопасности информации*** — *действие или событие*, которое может привести к *разрушению, искажению или несанкционированному использованию* информационных ресурсов (т.е. к утечке, модификации и утрате), включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.
- ***Система защиты*** — это совокупность (комплекс) специальных *мер правового (законодательного) и административного характера, организационных мероприятии, физических и технических (программно-аппаратных) средств защиты, а также специального персонала*, предназначенных для обеспечения безопасности информации, информационных технологий и автоматизированной системы в целом.

Для построения эффективной системы защиты необходимо провести следующие ***работы:***

1) *определить угрозы* безопасности информации;
2) *выявить возможные каналы утечки* информации и несанкционированного доступа (НСД) к защищаемым данным;
3) *построить модель* потенциального *нарушителя*;
4) *выбрать соответствующие меры*, методы, механизмы и *средства защиты*;
5) *построить* замкнутую, комплексную, эффективную *систему защиты*, проектирование которой начинается с проектирования самих АС и технологий.

*При **предпроектномм обследовании** объекта:*

- *устанавливается* наличие секретной (конфиденциальной) информации в разрабатываемой САПР, оценивается уровень ее конфиденциальности и объем;
- *определяются* режимы обработки информации (диалоговый, телеобработка и режим реального времени), состав комплекса технических средств и т.д.;
- *анализируется* возможность использования имеющихся на рынке сертифицированных средств ЗИ;
- *определяется степень участия* персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности;
- *определяются мероприятия* по обеспечению режима секретности на стадии разработки.

2. Виды угроз безопасности в САПР

Основными видами угроз безопасности информационных систем и информации (угроз интересам субъектов информационных отношений) являются:

- *стихийные* бедствия и аварии (наводнение, ураган, пожар и т.п.);
- *сбои и отказы* оборудования (технических средств) САПР;
- последствия *ошибок проектирования и разработки компонентов* САПР (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- *ошибки эксплуатации* (пользователей, операторов и другого персонала);
- *преднамеренные действия* нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Угрозы безопасности можно классифицировать по:

По результатам акции:

1) угроза утечки;

2) угроза модификации;

3) угроза утраты.

По нарушению свойств информации:

а) угроза нарушения конфиденциальности обрабатываемой информации;

б) угроза нарушения целостности обрабатываемой информации;

в) угроза нарушения работоспособности системы (отказ в обслуживании), т.е. угроза доступности.

По природе возникновения:

1) естественные; 2) искусственные.

- ***Естественные угрозы*** — это угрозы, вызванные воздействиями на САПР и ее элементы объективных физических процессов или стихийных природных явлений.

Основные непреднамеренные искусственные угрозы САПР *(действия, совершаемые случайно, по незнанию, невнимательности или халатности, но без злого умысла):*

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное включение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;

8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими угрозу для работоспособности системы и безопасности информации;

10) игнорирование организационных ограничений (установленных правил) при ранге в системе;
11) вход в систему в обход средств зашиты (загрузка посторонней операционной системы со сменных носителей и т.п.);
12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
13) пересылка данных по ошибочному адресу абонента (устройства);
14) ввод ошибочных данных;
15) неумышленное повреждение каналов связи.

Основные ***преднамеренные искусственные угрозы*** характеризуются возможными путями умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

а) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.);

б) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

в) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

г) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

д) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

е) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

ж) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводка активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

з) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

и) хищение носителей информации (флэш-карт, микросхем памяти, запоминающих устройств и персональных ЭВМ);
к) несанкционированное копирование носителей информации;
л) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
м) чтение остатков информации из оперативной памяти и с внешних запоминающих устройств;
н) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных операционных систем и систем программирования;
о) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т.п.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

п) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, адрес в системе связи, аппаратный блок кодирования и т.п.;

р) вскрытие шифров криптозащиты информации;

с) внедрение аппаратных спецвложений, программ «закладок» и «вирусов» («троянских коней» и «жучков»), т.е. таких участков программ, которые позволяют преодолеть систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации;

т) незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

у) незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

3. Методы и средства защиты информации

Проблема создания *системы защиты информации включает две взаимодополняющие задачи:*

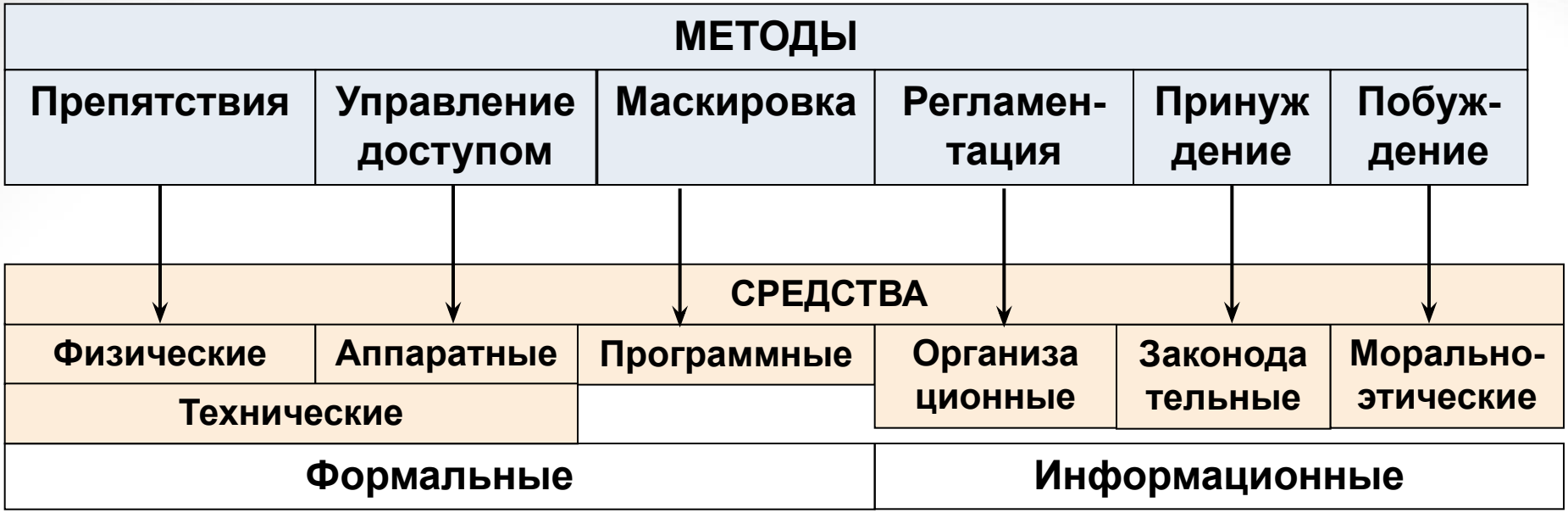
1) *разработка* системы защиты информации (ее синтез);

2) *оценка* разработанной системы защиты информации.

Вторая задача решается путем анализа ее технических характеристик с целью установления, удовлетворяет ли система защиты, информации комплексу требований к данным системам.

Такая задача в настоящее время решается почти исключительно экспертным путем с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Методы и средства обеспечения безопасности информации в САПР



Препятствия — методы физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом - метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств). Управление доступом включает в себя следующие ***функции защиты***:

- *идентификацию* пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- *опознание* (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- *проверку полномочий* (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- *разрешение* и создание условий работы в пределах установленного регламента;
- *регистрацию* (протоколирование) *обращений* к защищаемым ресурсам;
- *регистрацию* (сигнализация, отключение, задержка работ, отказ в запросе) *при попытках несанкционированных действий*.

- ***Маскировка*** — метод защиты информации путем ее криптографического закрытия. Этот метод широко применяется как при обработке, так и при хранении информации, в том числе на мобильных носителях информации. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.
- ***Регламентация*** — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.
- ***Принуждение*** — метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации *под угрозой* материальной, административной или *уголовной ответственности*.
- ***Побуждение*** — метод защиты, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Основные средства защиты

1. *Технические средства*
2. *Физические средства*
3. *Программные средства*
4. *Организационные средства*
5. *Морально-этические средства*
6. *Законодательные средства*

Основным средством защиты от вирусов служит ***архивирование***.

Другие методы заменить его не могут, хотя и повышают общий уровень защиты. Архивирование необходимо делать *ежедневно*. Архивирование заключается в создании копий используемых файлов и систематическом обновлении изменяемых файлов.

В целях профилактики для защиты от вирусов рекомендуется:

- работа с флэш-картами, *защищенными от записи*;
- минимизация периодов доступности мобильных носителей информации (МНИ) для записи;
- разделение МНИ между конкретными ответственными пользователями;
- разделение передаваемых и поступающих МНИ;
- разделение хранения вновь полученных и эксплуатировавшихся ранее программ;
- проверка вновь полученного программного обеспечения на наличие в них вируса тестирующими программами;
- хранение программ на жестком диске в архивированном виде.

Чтобы избежать появления компьютерных вирусов

- не переписывать программное обеспечение с других компьютеров. Если это необходимо, то следует принять перечисленные выше меры;
- не допускать к работе на компьютере посторонних лиц, особенно если они собираются работать со своими МНИ;
- не пользоваться посторонними МНИ, особенно с компьютерными играми.

Типичные ошибки пользователя

- отсутствие надлежащей системы архивации информации;
- запуск полученной программы без ее предварительной проверки на зараженность и без установки максимального режима защиты винчестера с помощью систем разграничения доступа и запуска резидентного сторожа;
- выполнение перезагрузки системы при наличии установленной в USB входе флэш-накопителя (при этом BIOS делает попытку загрузиться именно с этого накопителя, а не с винчестера; в результате, если флэшка заражена бутовым вирусом[1], происходит заражение винчестера);
- прогон всевозможных антивирусных программ, без знания типов диагностики одних и тех же вирусов разными антивирусными программами;
- анализ и восстановление программ на зараженной операционной системе.

[1] Отличительной особенностью ***бутового вируса*** является инфицирование загрузочного (бут - сектора) магнитного носителя (гибкого или жесткого диска).

Логотипы наиболее распространенных фирм производителей антивирусного ПО.

- Среди наиболее популярных у российских пользователей антивирусных пакетов назовем программы: Norton Antivirus, Антивирус Касперского, Dr.Web, и Secret Net Studio («Код Безопасности»).
- Существуют программы-фильтры, проверяющие, имеется ли в файлах (на указанном пользователем диске) специальная для данного вируса комбинация байтов. Используется также специальная обработка файлов, дисков, каталогов — ***вакцинация***: запуск программ-вакцин, имитирующих сочетание условий, в которых начинает работать и проявляет себя данный тип вируса.

П А М Я Т К А
по обеспечению режима безопасности и эксплуатации оборудования, установленного в защищаемом помещении (Примерный текст)

1. Ответственность за режим безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

2. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением (специалистом) по защите информации предприятия.

3. В нерабочее время помещение должно закрываться на ключ.

4. В рабочее время, в случае ухода руководителя, помещение должно закрываться на ключ или оставляться под ответственность лиц назначенных руководителем подразделения.

5. При проведении конфиденциальных мероприятий бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.

П А М Я Т К А
по обеспечению режима безопасности и эксплуатации оборудования, установленного в защищаемом помещении (Продолжение)

6. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и др. оборудования, установленного в помещении.

7. Запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой и транкинговой связи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком, спикерфоном и имеющих выход в городскую АТС, следует отключать эти аппараты на время проведения конфиденциальных мероприятий.

8. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, и служба безопасности предприятия.

9. Периодический контроль эффективности мер защиты помещения осуществляется специалистами по защите информации.

4. Аппаратно-программный модуль доверенной загрузки (АПМДЗ)

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***:

1. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
2. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
3. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

4.1. Назначение АПМДЗ

- ***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*:

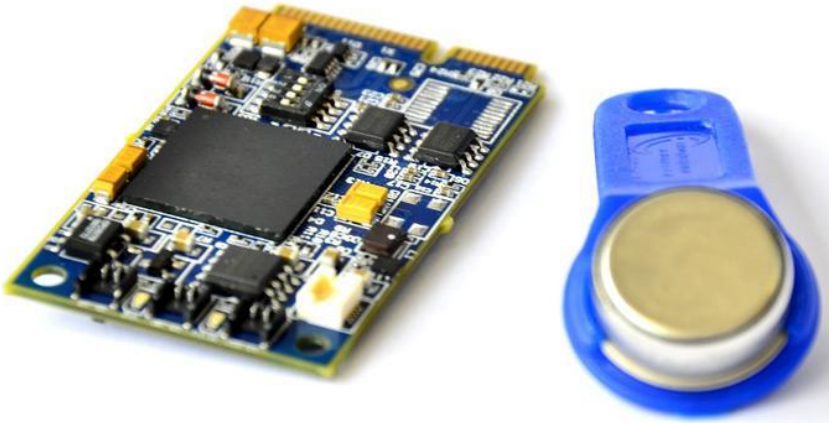
• ***программно-аппаратные комплексы (ПАК) семейства "Соболь"*** разработки "Код Безопасности";

• ***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".*

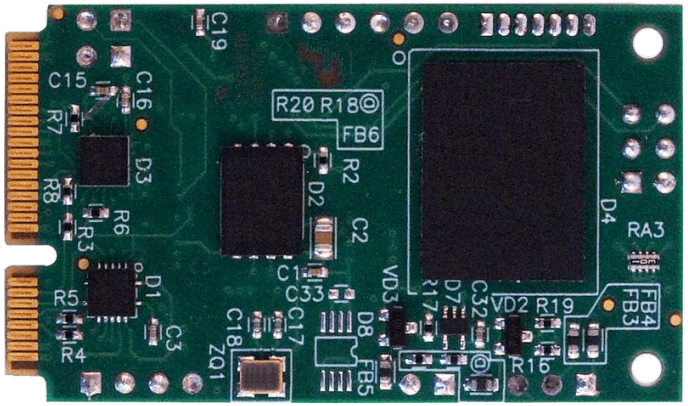
В данном вопросе лекции будут рассмотрены основные возможности и характеристик АПМДЗ на примере устройств семейства "Цезарь".

Внешний вид плат АМПДЗ.



ПАК «Соболь»

АМДЗ «Аккорд»



АПМДЗ «Криптон-Замок»

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 данной ПЭВМ требуемую политику безопасности независимо от программного обеспечения (в том числе и операционной системы), установленного на ПЭВМ.*

4.2. Состав изделия

Рис. 4.2. Типовой состав АМПДЗ семейства «Соболь».

4.2. Состав изделия

Рис. 4.3. Типовой состав АМПДЗ семейства «Соболь».

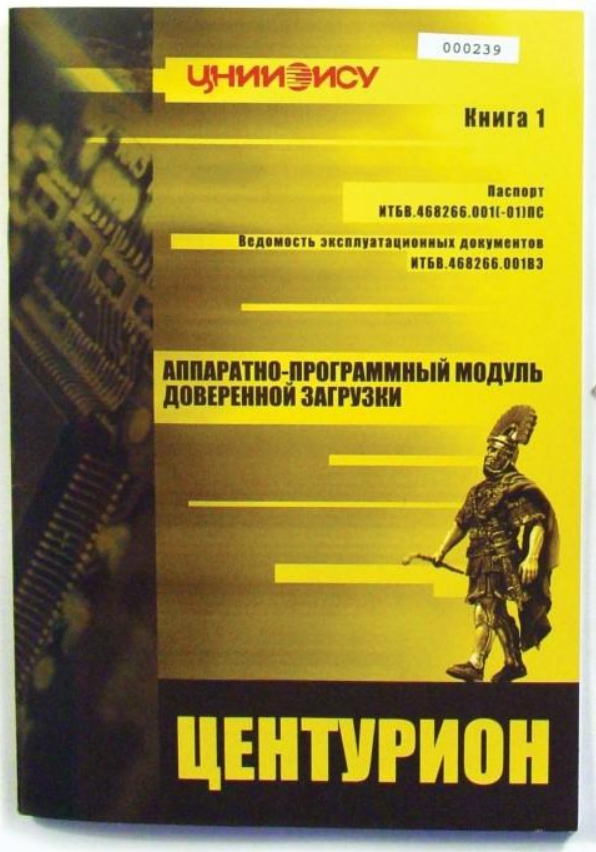
В типовой состав АПМДЗ входят следующие функциональные узлы:

- ***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 аутентифицирующие носители пользователей (АНП).

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

Рис. 4.4. 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. 4.5. Внешний вид платы АМПДЗ «Цезарь».

- **Рис. 4.6. Внешний вид платы АМПДЗ 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.

4.4. 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 контрольного вектора носителя 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 персонального идентификационного кода 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.

5. 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 , Windows Server 2012/2008/2003 и др.

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.

5.1. 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;

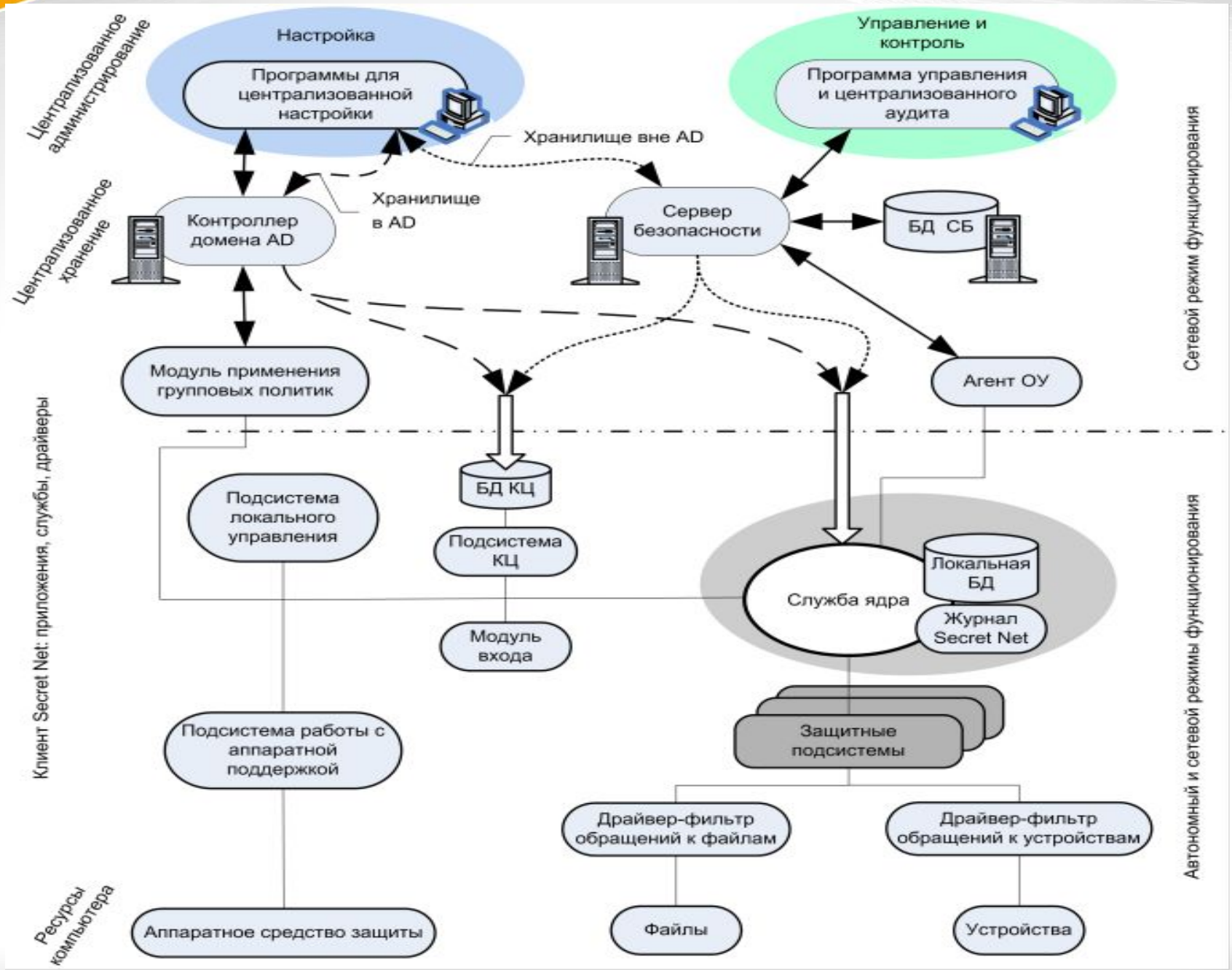
- контроль подключения и изменения устройств компьютера;
- функциональный контроль ключевых компонентов SecretNet;
- защита содержимого дисков при несанкционированной загрузке;
- уничтожение (затирание) содержимого файлов при их удалении;
- теневое копирование выводимой информации;
- регистрация событий 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.

5.2. 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.

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*:

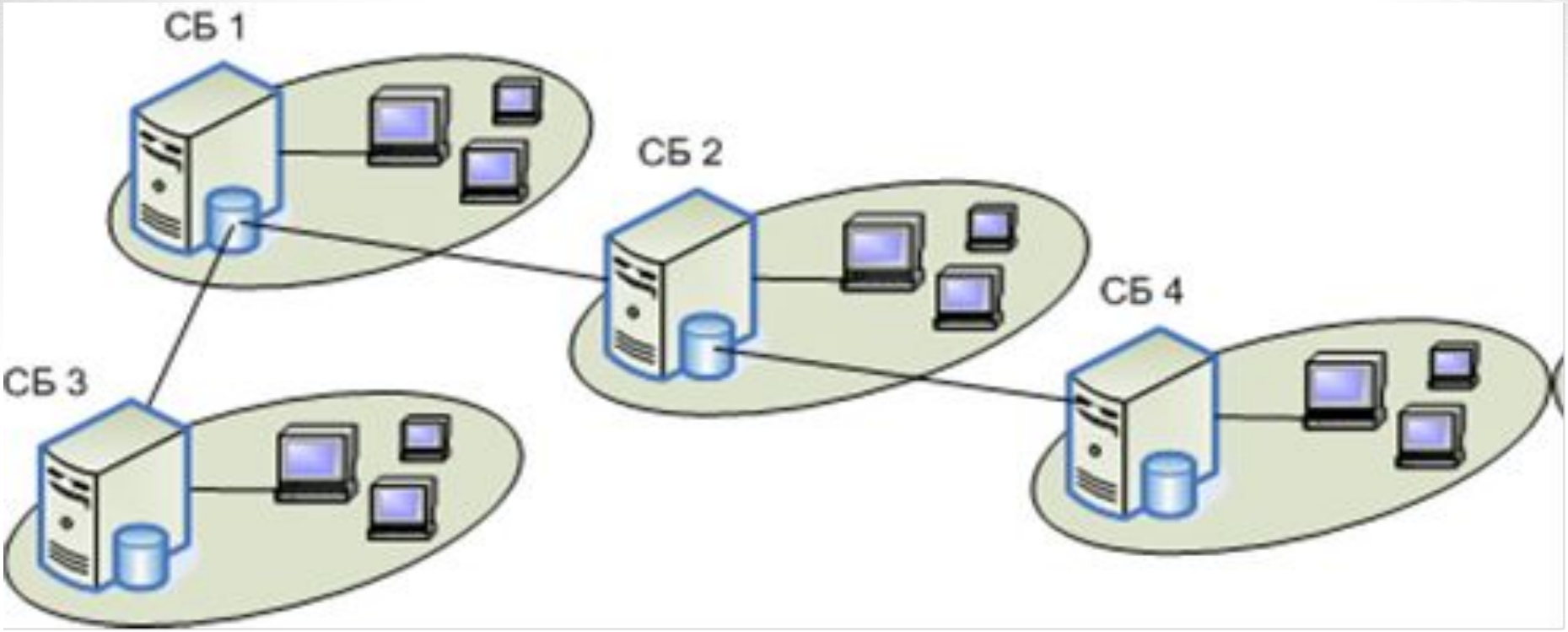
- модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам;
- модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
- драйверы устройств аппаратной поддержки (если они необходимы).

5.3. 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).
ТМ устройство сенсорной памяти Touch Memory.

Контрольные вопросы

1. В каком качестве по отношению к определенной информации могут выступать субъекты?
2. Доступность информации – это…?
3. Целостность информации – это…?
4. Конфиденциальность информации – это…?
5. Безопасность информации – это…?
6. Модификация информации – это…?
7. СЗИ – это…?
8. Какие задачи решаются при создании системы защиты информации?
9. Что называется управлением доступом в СЗИ?
10. Что называется маскировкой в СЗИ?
11. Что называется принуждением в СЗИ?
12. Что называется побуждением в СЗИ?
13. Какие средства относятся к основным средствам защиты в СЗИ?
14. Основным средством защиты от вирусов служит…?
15. Перечислите основные принципы «Концепция защиты СВТ и АС от НСД к информации»?
16. Для чего предназначен АПМДЗ?
17. Какие функциональные узлы входят в типовой состав АПМДЗ?
18. Укажите длину уникального номера носителя (УНН) для Touch Memory (ТМ) АПМДЗ «Цезарь»?
19. Укажите длину пароля для АПМДЗ «Цезарь»?
20. Укажите максимальное количество пользователей, допускаемых к ПЭВМ с АПМДЗ «Цезарь»?
21. Перечислите основные принципы функционирования АПМДЗ?
22. В каком состоянии может находиться АПМДЗ?
23. В эксплуатационном состоянии АПМДЗ различается два режима:...?
24. Для чего предназначен режим инициализации АПМДЗ?
25. Для чего предназначен технологический режим АПМДЗ?
26. Для чего предназначена система Secret Net?
27. В каких режимах может функционировать система Secret Net?
28. Система Secret Net состоит из отдельно устанавливаемых программных средств:…?
29. В каком режиме функционирования используется компонент "Модификатор схемы Active Directory" системы Secret Net?
30. Какие основные компоненты и подсистемы включает Secret Net Клиент?
31. Какие программные средства должны быть установлены в системе Secret Net для централизованного управления в сетевом режиме?
32. По какому принципу строится сетевая структура системы Secret Net?