МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ ИНФОРМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра ИБ

**ПАСОИБ**

Выполнил:

студент группы БИ-41,

Пекунов Е.А.

.

Йошкар-Ола

2017 г

**1.Аккорд**

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера — до загрузки операционной системы. Контроллеры семейства «Аккорд-АМДЗ» обеспечивают доверенную загрузку ОС, поддерживающих наиболее распространенные файловые системы, включая: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX. Это, в частности, ОС семейств MS DOS, Windows, QNX, OS/2, UNIX, LINUX, BSD и др.

«Аккорд-АМДЗ», как правило, применяется в следующей конфигурации:

контроллер («Аккорд-АМДЗ») — представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы СВТ (РС). Контроллер является универсальным, не требует замены при смене используемого типа операционной системы (ОС);

съемник информации с контактным устройством, обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя;

персональный идентификатор пользователя— специальное устройство, содержащее уникальный признак пользователя, с которым зарегистрированный пользователь входит в систему и который используется системой для определения его прав, а также для регистрации факта доступа и характера выполняемых им работ или предоставляемых ему услуг.

Количество и тип идентификаторов, модификация контроллера и съемника оговариваются при поставке комплекса. Персональные идентификаторы и съемники информации заказываются отдельно.

«Аккорд-АМДЗ» может быть реализован на различных контроллерах, предназначенных для работы с разными шинными интерфейсами СВТ. При этом его базовая функциональность всегда остается одинаковой (вне зависимости от типа контроллера) и соответствует заявленной и отраженной в конструкторской и эксплуатационной документации.

Сертифицирован ФСБ России. Сертификат подтверждают, что Аккорд-АМДЗ соответствует уровню контроля аппаратно-программному защиты от НСД. 3 класс защищенности.

Долго устанавливали, проблемная реализация ИПС, не могли записать пароли для пользователей, так же был немного дефектный ключ. Не смогли сделать цифровую подпись документа.

**2)АПМДЗ Соболь (разработчик «Код Безопасности»)**

Соболь является средством защиты информации от несанкционированного доступа на персональных компьютерах. Соболь выполняет роль аппаратно-программного модуля доверенной загрузки. ПАК Соболь предназначен для защиты конфиденциальной информации, информации, содержащей сведения, составляющие государственную тайну со степенью секретности "совершенно секретно" включительно или относящейся к персональным данным.

ПАК Соболь выполняет следующие функции безопасности:

Блокирует попытки загрузки ОС со съемных носителей. После успешной загрузки штатной копии ОС доступ к этим устройствам восстанавливается. Запрет на загрузку распространяется на всех пользователей компьютера, за исключением администратора.

Идентифицирует и аутентифицирует пользователей.

Выполняет контроль целостности файлов и секторов жесткого диска (до загрузки ОС). Используемый в комплексе Соболь механизм контроля целостности позволяет контролировать неизменность файлов и физических секторов жесткого диска до загрузки операционной системы.

Выполняет роль сторожевого таймера. Механизм сторожевого таймера обеспечивает блокировку доступа к компьютеру при условии, что после включения компьютера и по истечении заданного интервала времени управление не передано расширению BIOS комплекса "Соболь"

Регистрирует события безопасности системы в собственной энергонезависимой памяти.

ПАК Соболь поддерживает работу со следующими операционными системами:

ОС семейства Windows (поддержка как 32, так и 64 битных)

ОС МСВС 3.0

Trustverse Linux XP Desktop 2008 Secure Edition

FreeBSD версии 5.3, 6.2, 6.3 или 7.2, 8.0, 8.1, 8.2

VMWare ESX 3.5 – 4.0

ПАК Соболь поддерживает файловые системы: NTFS, FAT 32, FAT 16, UFS, EXT3, EXT2.

Поддержка различных типов идентификаторов (Rutoken, eToken, "таблетки" DS iButton)

Возможность программной инициализации комплекса

Возможности по администрированию

Для настройки ПАК Соболь администратор имеет возможность:

Определять минимальную длину пароля пользователя;

Определять предельное число неудачных входов пользователя;

Добавлять и удалять имена пользователей;

Блокировать работу пользователя на компьютере;

Создавать резервные копии персонального идентификатора администратора.

Программно инициализировать комплекс.

Сертифицирован ФСБ России. Сертификат подтверждают, что АПМДЗ Соболь соответствует уровню контроля аппаратно-программному модулю доверенной загрузки (АПМДЗ) по классу 1Б. Это подтверждает факт того, что АПМДЗ Соболь может быть использован в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Не было возможности сделать ИПС из-за пробной версии продукта.

**3)АПМДЗ Криптон-Замок (разработчик «АНКАД»)**

«КРИПТОН-ЗАМОК» является одной из современных программно-аппаратных систем для защиты информации. «КРИПТОН-ЗАМОК» представляет собой сертифицированные комплексы программно-аппаратных средств, которые предназначены для обеспечения разграничения и контроля доступа пользователей к техническим средствам вычислительной сети, то есть серверы и рабочие станции, на которых обрабатывается информация даже с высоким грифом секретности. Данный комплекс программно-аппаратных средств обладает шестью основными возможностями:

1. блокировка компьютера при несанкционированном доступе;

2. создание нескольких профилей защиты и надежное разграничение ресурсов компьютера;

3. наличие аппаратного датчика случайных чисел;

4. идентификация пользователя до запуска BIOS компьютера и двухфакторная аутентификация пользователя;

5. накопление и ведение электронного журнала событий, причем в собственной энергонезависимой памяти;

6. подсчет эталонных значений контрольных сумм объектов и проверка текущих значений контрольных сумм .

«КРИПТОН-ЗАМОК» обладает и другими, не связанными с защитой персональных данных, возможностями: − организация бездисковых рабочих мест на основе встроенного флешдиска; − защита компьютера от нештатного электрического воздействия на тракт ввода ключевой информации; − инициализация устройств шифрования (сетевых шифраторов, абонентских шифра- торов, шифраторов жестких дисков серии КРИПТОН); − управление загрузкой операционной системы с жесткого диска; − контроль целостности загружаемой программной среды; − аппаратная защита от несанкционированной загрузки операционной системы с гибкого диска, CD-ROM, DVD-ROM, USB устройств. 4 Стоит отметить, что функции «КРИПТОН-ЗАМОК», связанные с управлением аппаратными шифраторами данного семейства «КРИПТОН» и его многофункциональным программным интерфейсом, обусловливают возможность построения на базе этой программно- аппаратной системы разнообразных комплексных решений по обеспечению безопасности систем компьютера

Преимущества программно-аппаратной системы защиты информации «КРИПТОН-ЗАМОК». К ним относятся: − наличие аппаратного датчика случайных чисел; − организация удаленного централизованного управления; − возможность разрешить некоторым пользователям осуществлять загрузку операционной системы с накопителя на гибком магнитном диске (НГМД) или CD ROM; − применение специального шифр процессора для выполнения криптографических преобразований, что разгружает центральный процессор компьютера; − модульная структура, которая позволяет настраивать и дорабатывать изделия «КРИПТОН-ЗАМОК» под разнообразные требования заказчиков в соответствии с необходимой областью применения. В заключение можно сделать вывод, что программно-аппаратная система защиты ин- формации «КРИПТОН-ЗАМОК» – это одна из наиболее надежных и качественных программно-аппаратных систем защиты информации, которая, в свою очередь, обладает широким спектром возможностей для использования в различных областях, где необходимо защитить информации разного рода, от отдельных клиентов до ФСБ.

Сертифицирован ФСБ России. Сертификат подтверждают, что АПМДЗ Криптон соответствует уровню контроля аппаратно-программному модулю доверенной загрузки (АПМДЗ) по классу 1Б. Это подтверждает факт того, что АПМДЗ Криптон может быть использован в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

**4)Secret Net**

Secret Net — семейство продуктов, с помощью которых осуществляется защита от НСД (несанкционированного доступа) на рабочих станциях и серверах.

В Secret Net используется комплекс традиционных и дополнительных механизмов обеспечения защиты рабочих станций и серверов от несанкционированного доступа. Традиционными механизмами обеспечивается выполнение требований регуляторов по защите персональных данных, конфиденциальной информации и государственной тайны. Дополнительный функционал средств защиты от НСД повышает защищенность обрабатываемой на рабочих станциях и серверах информации.

Гибкие настройки СЗИ Secret Net и Secret Net LSP позволяют успешно решать стоящие перед организацией задачи разграничения доступа к информации, контроля устройств и потоков конфиденциальных данных и ряда других. Средства Secret Net, с помощью которых осуществляется защита от НСД серверов и ПК, совместимы с широкой линейкой ОС Windows и Linux/GNU. Продукты имеют механизмы централизованного мониторинга и управления, что позволяет внедрять их в организациях с большим парком различных устройств.

СЗИ от НСД Secret Net сертифицированы ФСТЭК и Минобороны России и могут применяться для защиты персональных данных, государственных информационных систем и конфиденциальной информации.

Установка, настройка ,создание контейнеров и привязывали их к пользователям, использование программы проблем не вызвало.

**5)Dallas Lock.**

Dallas Lock – система защиты информации от несанкционированного доступа, сертифицированная и позволяющая привести автоматизированные системы в соответствие требованиям законов РФ, стандартов и руководящих документов.

Dallas Lock имеет сертификат ФСТЭК, позволяющий использовать его для защиты конфиденциальной информации и государственной тайны в автоматизированных системах (АС) до класса защищенности 1Б включительно.

Возможности Dallas Lock:

Однофакторная или двухфакторная аутентификация пользователей

Контроль каналов распространения конфиденциальной информации

Позволяет выполнять очистку остаточной информации

Позволяет разграничить права доступа администраторов и пользователей к локальным и сетевым ресурсам

Позволяет разграничить доступ к сменным накопителям для предотвращения возможной утечки конфиденциальной информации.

Возможность администрирования рабочих мест удаленно

Возможность работы с помощью сервера терминального доступа

Разграничение прав по мандатному и дискреционному принципу

Организация доверенной информационной среды

Способность создать замкнутую программную среду

Имеет трехуровневую систему управления безопасностью (компьютер-домен безопасности-лес безопасности), что позволяет применять Dallas Lock в организации с большим количеством филиалов

Контроль целостности ресурсов компьютера и программно-аппаратной конфигурации

Отсутствие обязательной аппаратной части

При использовании Сервера безопасности, возможность централизованно управлять политиками безопасности

Дает возможность проводить оперативный мониторинг и аудит действий пользователей

Проблем с документацией , установкой, настройкой и работой не было.

**Общие выводы**

В соответствии с удобством и пониманием использования и представленными возможностями было выбрано два наиболее оптимальных варианта:

- ПАК Аккорд;

-Dallas Lock.

Каждый продукт имеет свои плюсы и свои минусы.

Главный плюс Dallas Lock заключается в том, что возможна полноценная защита без использования дополнительных технических средств, что может быть очень важно для организации. Минус же кроется в том, что нет защиты аппаратной части АРМ, а также нет гарантий разработчика отсутствия конфликтов при использовании сторонних СЗИ, таких как АПМДЗ. Данное СЗИ имеет самую простую и понятную оболочку настройки по сравнению с другими СЗИ. На Secret Net в отличии от Dallas Lock имеет возможность использовать в качестве аппаратной защиты модули доверенной загрузки, такие как АПМДЗ Соболь или Secret Net Card. Использовании в паре с АПМДЗ Соболь позволяет использовать его для защиты конфиденциальной информации и государственной тайны в автоматизированных системах (АС) до класса защищенности 1Б включительно. Также колоссальным преимуществом Secret Net над другими СЗИ является возможность развёртывания на компьютерах под управлением Unix-подобных систем. Так же на ресурсах интернета, в отзывах использования была найдена статья об обходе правил разграничения доступа в средствах защиты от НСД, она осуществлялась в Dallas lock, с запуском файла через командную строку, у Secret Net отсутствует данная уязвимость.

|  |  |
| --- | --- |
| **СЗИ** | **КЗ** |
| Аккорд АМДЗ | 1Д |
| АПМДЗ Соболь | до 1Б включительно |
| АПМДЗ Криптон-Замок | - |
| Secret Net | до 1Б включительно |
| Dallas Lock | 1Б |