ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 2015 г.

Автор: преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 11

Тема: «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗИ»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
протокол № __ «____» _____ 201_ г.

Санкт-Петербург
201_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Понятие средства ЗИ – 30 мин.
2. Классификация средств ЗИ – 20 мин.
3. Краткая характеристика средств ЗИ – 30 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области программно-аппаратных средств ЗИ.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на программно-аппаратных средствах ЗИ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите основные программно-аппаратные средства ЗИ?
2. В чем заключается суть механизма разграничения доступа?
3. Охарактеризуйте систему Dallas Lock?
4. Охарактеризуйте страж NT?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 11

Раздел III Защита от несанкционированного доступа к ресурсам вычислительных систем

В. 1. Программные средства защиты информации

На основе программно-аппаратных методов защиты создаются программно-аппаратные средства защиты, которые могут сочетать в себе не один, а несколько методов защиты информации. Простота реализации и администрирования, высокая эффективность применения, приемлемые цены делают эти методы, и средства защиты на их основе, очень привлекательными для пользователей во всём мире.

В соответствии с ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» (дата введения 1.07.97 г.) *под средством защиты информации* понимают – техническое, программное средство, вещество и/или материал, предназначенное или используемое для защиты информации. А *под защитой информации* – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

К аппаратным – относятся средства защиты информации, входящие в состав аппаратуры АС.

Программными называются средства защиты информации, функционирующие в составе программного обеспечения АС.

Рынок средств информационной безопасности представлен многочисленными продуктами, реализующими различные технологии защиты. В таблице 3.1. приведены основные средства защиты информации автоматизированных систем. Многие из этих средств имеют действующие сертификаты ФЭСТЭК России.

Программные средства защиты информации

Программными СЗИ называются специальные *программы, входящие в состав программного обеспечения АС для решения в них (самостоятельно или в комплекте с другими средствами) задач защиты*. Программные СЗИ являются непременной и важнейшей частью механизма защиты современных АС. Такая их роль определяется следующими достоинствами: универсальностью, гибкостью, простой реализацией, надежностью, возможностью модификации и развития.

При этом под *универсальностью* понимается возможность решения программными СЗИ большого числа задач защиты.

Под *надежностью* понимается высокая программная устойчивость при большой продолжительности непрерывной работы и удовлетворение высоким требованиям и достоверности управляющих воздействий при

наличии различных дестабилизирующих факторов. Программные возможности изменения и развитияпрограммных СЗИ определяются самой их природой.

Существенным недостатком программных СЗИ является возможность их реализации только в тех структурных элементах АС, где имеется процессор, хотя функции защиты могут реализовываться, осуществляя безопасность других структурных элементов. Помимо того, программным СЗИ присущи следующие ***недостатки***:

необходимость использования времени работы процессора, что ведет к увеличению времени отклика на запросы и, как следствие, к уменьшению эффективности ее работы;

уменьшение объемов оперативной памяти (ОП) и памяти на внешних запоминающих устройствах (ПВЗУ), доступной для использования функциональными задачами;

возможность случайного или умышленного изменения, вследствие чего программы могут не только утратить способность выполнять функции защиты, но и стать дополнительными источниками угрозы безопасности;

ограниченность из-за жесткой ориентации на архитектуру определенных типов ЭВМ (даже в рамках одного класса) — зависимость программ от особенностей базовой системы ввода/вывода, таблицы векторов прерывания и т.п.

Для ***организационного построения программных СЗИ*** наиболее характерной является тенденция разработки комплексных программ, выполняющих целый ряд защитных функций, причем чаще всего в число этих функций входит опознавание пользователей, разграничение доступа к массивам данных, запрещение доступа к некоторым областям ОП и т.п. **Достоинства** таких программ очевидны: каждая из них обеспечивает решение некоторого числа важных задач защиты. Но им присущи и существенные **недостатки**, предопределяющие необходимость критической оценки сложившейся практики разработки и использования программных средств защиты. Первый и главный недостаток состоит в *стихийности развития программ защиты*, что, с одной стороны, не дает гарантий полноты имеющихся средств, а с другой – не исключает дублирования одних и тех же задач защиты. Вторым существенным недостатком является *жесткая фиксация в каждом из комплексов программ защитных функций*. Наконец, можно выделить еще один большой недостаток – ориентация подавляющего большинства имеющихся программных средств на конкретную среду применения (тип ЭВМ и операционную среду).

Отсюда вытекают три принципиально важных ***требования к формированию программных СЗИ***: **функциональная полнота**, **гибкость** и **унифицированность использования**.

Что касается первого требования, то, как нетрудно убедиться, приведенный выше перечень программных средств составлен именно с таким расчетом, чтобы возможно более полно охватить все классы задач защиты.

Удовлетворение остальным двум требованиям зависит от форм и способов представления программ защиты. Анализ показал, что наиболее полно требованиям гибкости и унифицированности удовлетворяет следующая совокупность принципов: *сквозное модульное построение*, *полная структуризация*, *представление на машинно-независимом языке*.

Принцип *сквозного модульного построения* заключается в том, что каждая из программ любого уровня (объема) должна представляться в виде системы возможных модулей, причем каждый модуль любого уровня должен быть полностью автономным и иметь стандартные вход и выход, обеспечивающие комплексирование с любыми другими модулями. Нетрудно видеть, что эти условия могут быть обеспечены, если программные комплексы будут разрабатываться по принципу “сверху вниз”, т.е. в соответствии с принципом *полной структуризации*.

Представление на машинно-независимом языке предопределяет, что представление программных модулей должно быть таким, чтобы их с минимальными усилиями можно было включить в состав программного обеспечения любой АС.

В настоящее время имеются алгоритмические языки высокого уровня, полностью соответствующие этим требованиям. Общепринятой классификации программных СЗИ в настоящее время не существует. Однако при описании программ защиты обычно придерживаются деления их по функциональному признаку, т.е. по выполняемым функциям защиты. При этом по мере развития форм и способов использования вычислительной техники функции программной защиты расширяются. С учетом названных принципов можно использовать классификацию, приведенную на рис.1.

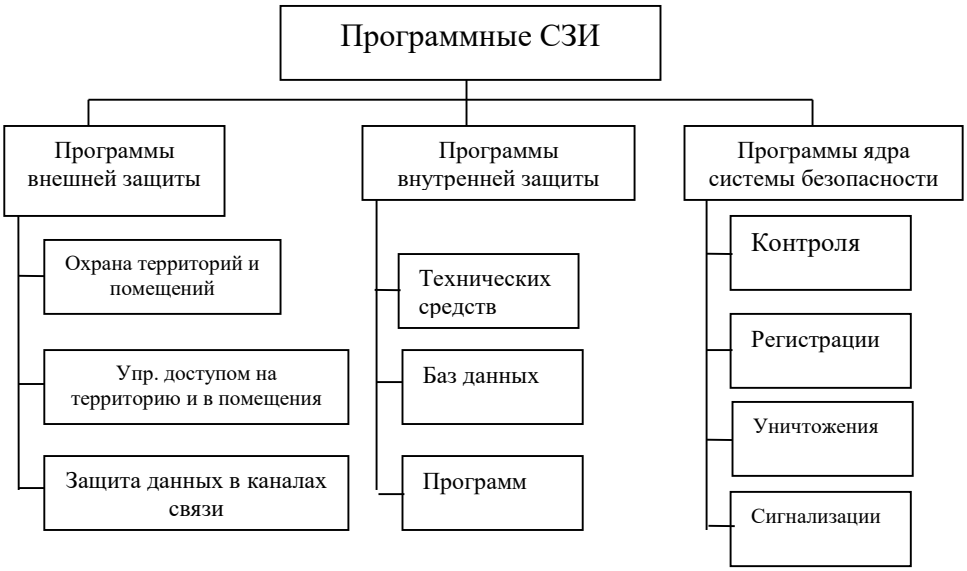

Рис.1. Классификация программных СЗИ

При этом под *внешней* защитой понимается совокупность средств, методов и мероприятий, направленных на защиту территории, на которой расположены здания вычислительных центров, и помещений, в которых расположены их элементы. Понятие *внутренней* защиты охватывает

совокупность средств, методов и мероприятий, направленных на ЗИ, обрабатываемой в АС. В состав *ядра системы безопасности* входят программы, обеспечивающие защиту самой СЗИ.

В. 2. Классификация средств ЗИ.

Таблица 3.1. Средства защиты информации

Средства защиты информации автоматизированных систем			
наименование	**тип**		**пример**
межсетевые экраны	сегментные		*Check Point* Next Generation Firewall*; *ОАО Элвис+* Застава**, *ОАО ИнфоТеКС* VIPNet Office Firewall**, *ООО АМИКОН* ФПСУ-IP**
	встраиваемые		*Network –1* Cyberwall-Plus
	персональные		*ОАО ИнфоТеКС* VIPNet Personal Firewall**, *McAfee* Personal Firewall; *Agnitum* Outpost Firewall
системы разграничения доступа	сетевые		*НИП информзащита* Secret Net**; *ГУП СЦПС «Спектр»* Спектр-Z(M)**, *ОКБ САПР* Аккорд**, *НИИ ПУИиМ академии ВН* Страж NT 3.0**, *Кон фидент* Dallas Lock**
	локальные		
	системы идентификации и аутентификации (СИА)		*НИП Информзащита* Соболь-PCI**, *ОКБ САПР* Аккорд-АМДЗ**, *АНКАД* КРИПТОН-Замок/ PCI**
системы построения VPN	на основе	сетевых ОС	Windows NT, XP, Vista, 7, 8, 8.1, 10 и др.
		маршрутизаторов	*Cisco* IOS 12.x*
		МЭ	*Check Point* FireWall-1* *Cisco* PIX 535*
		специализированного ПО	*Digital Equipment* Alta Vista Tunnel 97; *ОАО Элвис+* Застава 6**, *ОАО ИнфоТеКС* VipNet Office**
		специализированных аппаратно-программных средств	*НИП Информзащита* Континент – К**; *МО ПНИЭИ* Шифратор IP пакетов
системы обнаружения атак (СОА)	средства антивирусной защиты	рабочих станций	*ЗАО ДиалогНаука* Антивирусный пакет Dr.Web Security Space**, *ЗАО Лаборатория Касперского* Антивирус Касперского 15/16**, *SYMANTEC* Norton Antivirus Suite v.12**
		серверов ЛВС	
		МЭ – антивирусных шлюзов	*ЗАО Лаборатория Касперского* Антивирус Касперского для CheckPoint Firewall**
	СОА на уровне сети		*ISS* RealSecure Network Engine, NFR, Snort
	СОА на уровне хоста		*ISS* RealSecure System Agent, RealSecure Desktop
средства анализа защищённости	сетевого уровня		*ISS* Internet Scanner, Wireless Scanner, Network Mapper, *Symantec* NetRecon, Nessus, *Positive Technologies* XSpider 7.0
	системного уровня		*ISS* System Scanner, *Symantec* Enterprise Security Manager
			ISS Database Scanner
средства защиты электронных документов	программно-аппаратный комплекс		удостоверяющий центр КриптоПро

Средства защиты информации автоматизированных систем		
наименование	**тип**	**пример**
	средства заверения электронных документов	*ЛАН Крипто* Нотариус, Веста, КриптоБанк, КриптоПро (CSP,TLS)

Курсивом выделены названия компаний производителей.

* На отдельные изделия имеется сертификат Гостехкомиссии России.

** На производство данного изделия имеется сертификат Гостехкомиссии РФ (использована информация с Иинтернет-сайта www.lissi.ru).

Условно можно выделить две категории средств защиты – традиционные и все остальные. К *традиционным средствам защиты* можно отнести *системы разграничения доступа* и *межсетевые экраны.* Первые средства реализуют разграничение доступа конкретных пользователей к ресурсам конкретного компьютера или всей сети, а вторые – разграничивают доступ между двумя участками сети с различными требованиями по безопасности.

В. 3. Краткая характеристика средств ЗИ.

Система защиты информации от НСД Страж NT 3.0 предназначена для комплексной многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС) и информационных системах персональных данных. СЗИ от НСД Страж NT (версия 3.0) функционирует в среде 32-х и 64-разрядных операционных систем MS Windows 2000 (Server и Professional), MS Windows XP (Professional и Home Edition), MS Windows Server 2003, MS Windows Vista, MS Windows 7, MS Windows Server 2008, MS Windows Server 2008 R2 и устанавливается как на автономных рабочих местах, так и на рабочих станциях и серверах локальной вычислительной сети.

СЗИ от НСД Страж NT 3.0 имеет сертификат ФСТЭК России №2145.

Основные возможности:

- идентификация и аутентификация пользователей при входе в систему по идентификатору и паролю;
- блокировка клавиатуры на время загрузки операционной системы (за исключением администратора безопасности);
- управление запуском всех системных компонентов, включая драйверы, службы и прикладные программы пользователей;
- создание изолированной программной среды для пользователей;
- дискреционный контроль доступа к ресурсам системы;
- мандатный контроль доступа к защищаемым ресурсам, в т.ч. прикладных программ;
- контроль потоков защищаемой информации;
- автоматическое затирание защищаемых файлов при их удалении;
- контроль целостности информационных массивов и программной среды.

ПАК Аккорд-Win32 К и ПАК Аккорд-Win64 К

Программно-аппаратные комплексы средств защиты информации(ПАК СЗИ) Аккорд-Win32 и Аккорд-Win64 предназначены для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам.

ПАК СЗИ работает на рабочих станциях, функционирующих под управлением ОС Windows NT/XP/Vista/7/8.

Реализует следующие функции:

- доверенная загрузка компьютера;

- идентификация/аутентификация пользователя;
- контроль целостности системной области диска, системных файлов, программ и данных;
- разграничение доступа пользователей к ресурсам компьютера;
- ведение протокола регистрируемых событий.

Dallas Lock – система защиты информации, в процессе её хранения и обработки, от несанкционированного доступа. Представляет собой программный комплекс средств защиты информации в автоматизированных системах.

СЗИ Dallas Lock может быть установлена на любые компьютеры, работающие под управлением ОС Windows. До версии системы 8.0 Dallas Lock поддерживаем 32-битные версии операционных систем, начиная с версии Dallas Lock 8.0 – 32- и 64-битные.

СЗИ Dallas Lock обеспечивает защиту стационарных, портативных и мобильных компьютеров как автономных, так и в составе локальной вычислительной сети, от несанкционированного доступа к информации.

Использование Dallas Lock в проектах по защите информации ограниченного доступа (конфиденциальная информация, в том числе персональные данные, и сведения, составляющие государственную тайну) позволяет привести автоматизированные системы, государственные информационные системы и обработку персональных данных в соответствие требованиям законов Российской Федерации, стандартов и руководящих документов.

СЗИ Dallas Lock позволяет в качестве средства опознгавания пользователей использовать аппаратные электронные идентификаторы:

- USB-Flash-накопители;
- электронные ключи Touch Memory (iButton);
- USB-ключи и смарт карты Aladdin eToken
- USB-ключи Рутокен;
- USB-ключи и смарт-карты JaCarta.

Система защиты информации от НСД «Аура 1.2.4»

«Аура 1.2.4» - СЗИ от НСД предназначена для комплексной защиты информации, обрабатываемой на ПЭВМ под управлением ОС семейства MS Windows 2000/XP/Vista/Server 2003/Server/2008.

СЗИ имеет сертификат ФСТЭК №2527.

СЗИ решает следующие основные задачи:

- усиленная аутентификация;
- контроль доступа к устройствам, файлам и папкам;
- управление печатью, автоматическая маркировка и учет документов;
- достоверное уничтожение информационных объектов;
- регистрация действий пользователя в системных журналах;
- блокировка консолей с помощью электронных ключей Rutoken, eToken и флеш-накопителей.
-

- Старший преподаватель 27 кафедры
- подполковник
- С.Краснов