ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 201_ г.

Автор: преподаватель 63 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 20

Тема: «ПЕРСПЕКТИВЫ И ТЕНДЕНЦИИ РАЗВИТИЯ ЗАЩИТЫ ИНФОРМАЦИИ»

по дисциплине: «Защита информации»

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

Санкт-Петербург
2015

Содержание занятия и время

ВСТУПИТЕЛЬНАЯ ЧАСТЬ – 5 МИН.
ОСНОВНАЯ ЧАСТЬ:
1. Краткий обзор дисциплины – 20 мин.
2. Проблемы обеспечения информационной безопасности отечественных информационных систем – 30 мин.
3. Перспективы и тенденции развития – 30 мин.

ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ – 3-5 МИН.

Цель лекции: Ознакомить курсантов с перспективами развития системы защиты информации.

Литература:

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. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

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 основных приказах МО РФ в области ЗИ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Назовите основные приказы МО РФ в области защиты информации?
2. Охарактеризуйте основные положения руководства утвержденного № 010 приказом МО РФ?
3. Охарактеризуйте основные положения инструкции утвержденной № 011 приказом МО РФ?

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

Сегодня у нас заключительная лекция по дисциплине «Защита информации». Итак, лекция № 20:

Слайд№1

«Перспективы и тенденции развития защиты информации в Космических войсках».

Цель занятия:

1. **закрепить ранее полученные знания путём краткого обзора дисциплины,**
2. **ознакомить вас с перспективами и тенденциями развития защиты информации в Космических войсках.**

Вопросы которые мы рассмотрим на сегодняшнем занятии:
(пока не записывайте, будем записывать по мере изучения вопроса)

1. **Краткий обзор дисциплины.**
2. **Проблемы обеспечения информационной безопасности отечественных информационных систем.**

Литература для самостоятельной подготовки:

1. Конспект лекций.
2. Директива Генерального штаба ВС РФ: «Концепция создания и оснащения базовыми информационными защищёнными компьютерными технологиями ВС РФ».
3. Директива Генерального штаба ВС РФ: «Концепция развития системы управления ВС РФ на период до 2016 года».
4. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. .Т. Тучкова, 2005. (стр. 144-146).

Актуальность данной темы занятия в том, что в настоящее время в Вооруженных Силах РФ применяется несколько десятков операционных систем (более 50) и еще большее количество систем управления базами данных. В сочетании с практически полным спектром аппаратных платформ данное обстоятельство обусловливает крайне низкий уровень совместимости эксплуатируемых объектов информационной инфраструктуры (ОИИ), сложность их общесистемной интеграции, проблемный характер многих вопросов, связанных с практической реализацией концепции единого информационного пространства Вооруженных Сил. Так, например, …

Основные недостатки присущие АРМ на базе ОС Windows NT + Secret Net

1. Не способность средства разграничения доступа «SecretNet» работать с ОС МСВС 3.0.

2. Невозможность осуществления постоянного полного аудита на сервере безопасности и АРМ администратора безопасности на объектах ВТ КВ состоящих из более чем 30 ПЭВМ. (Не справляется «SecretNet»).

Кроме того, в случае военных действий (например с США) точно не известно как поведут себя иностранные ОС, коды ядра которых закрыты и содержатся в секрете. Давайте на секунду представим, что будет, если все ОС Windows, которые есть в ВС РФ, хотя бы просто перестанут нормально работать?

Об этом мы поговорим во втором и третьем вопросе лекции, а сейчас **закрепим ранее полученные знания путём краткого обзора дисциплины.** Запишите

В.1. Краткий обзор дисциплины.

Всего мы с вами изучили 6 тем, напомню вкратце, о чём шла речь.

Тема 1. СУЩНОСТЬ ЗАЩИТЫ ИПО

Содержание предметной области защиты информации. Сущность и цели защиты ИПО. Основные положения доктрины информационной безопасности РФ. Угрозы ИПО и их классификация. Классификация источников угроз и уязвимостей безопасности

Под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-96].

По видам деятельности **предметная область «ЗИ»** подразделяется на три составляющие:

1. собственно *процесс ЗИ* как совокупность действий по применению методов (способов) и средств ЗИ;
2. *управление ЗИ* как совокупность целенаправленных воздействий органов управления на объекты защиты, силы и средства ЗИ;
3. *обеспечение ЗИ*, под которым понимается создание необходимых образовательных, научных, технических, информационных и других условий для реализации процесса ЗИ.

1. *Процесс ЗИ* характеризуются тремя составляющими:

- объектами защиты;
- угрозами, от которых необходимо обеспечить защиту объектов;
- методами (способами) и средствами защиты объектов от угроз.

Объекты защиты определяется тремя составляющими:

- информацией;
- носителем защищаемой информации;
- информационным процессом, протекающим на носителе, или физическим процессом, в котором участвует носитель защищаемой информации.

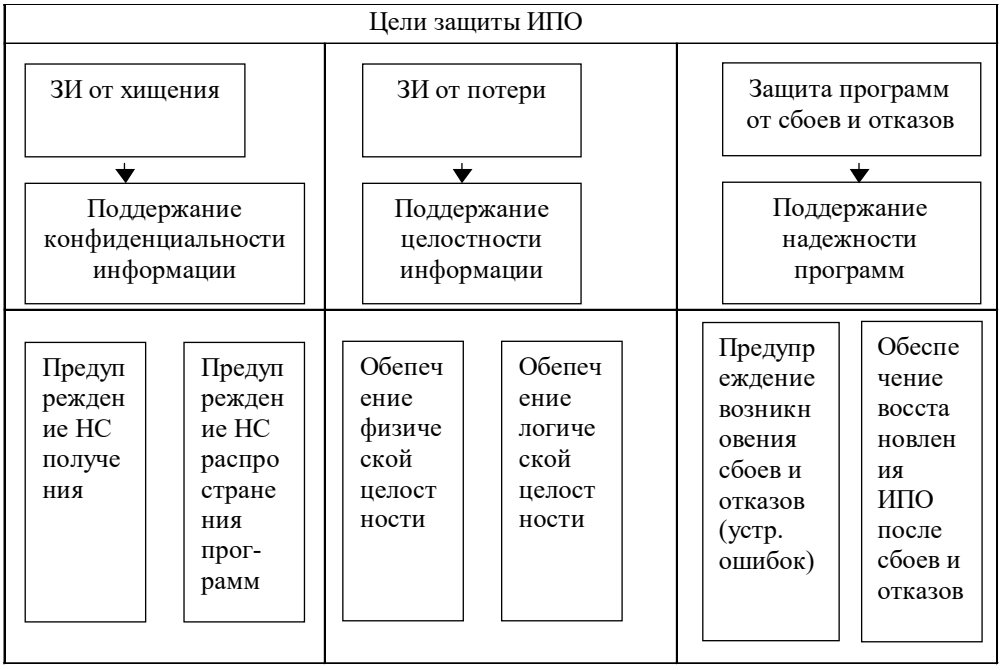
Угроза безопасности информации представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Защита ИПО – использование средств и методов, принятие мер и осуществление мероприятий с целью обеспечения безопасности хранимой и обрабатываемой информации, а также используемых в ВС программных средств.

Безопасность ИПО – это состояние информации, которое соответствует установленному статусу ее хранения и использования.

Понятие защиты имеет смысл, когда известны цели защиты, определяющие от чего надо защищать данные объекты.

Цели защиты ИПО можно представить в виде следующей схемы:



Основные положения доктрины информационной безопасности РФ *от 9 сентября 2000 г:*

Все национальные интересы РФ в информационной сфере, объединены в три основные группы:

1. Национальные интересы, связанные с соблюдением конституционных прав граждан в области получения информации и пользования ею;
2. Национальные интересы, связанные с развитием современных отечественных телекоммуникационных технологий;
3. Национальные интересы, связанные с развитием государственных информационных ресурсов.

Приведенные в доктрине выводы об угрозах развитию отечественной индустрии средств информатизации, телекоммуникации и связи, являются следствием уже примененной к России совокупности внешних воздействий информационного и экономического характера, а также внутренних причин.

Результатами этих воздействий можно считать следующие, приведенные в доктрине факторы:

- ограничение доступа Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации и информационных продуктов, а также противодействия усилению технологической независимости Российской Федерации от зарубежных стран в области информатизации;
- вытеснение с отечественного рынка средств информатизации, телекоммуникации и связи российских производителей;
- увеличение оттока квалифицированных кадров из России, их перехода в зарубежные компании;
- усиление зависимости духовной жизни общества, экономической и политической жизни страны от зарубежных информационных структур;

- снижение уровня образованности граждан, существенно осложняющего подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных.

Угроза безопасности информации представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Угрозы сами по себе не проявляются. Все угрозы могут быть реализованы (с помощью *методов реализации*) только при наличии каких-нибудь слабых мест – *уязвимостей,* присущих конкретной АС.

Уязвимость информационной системы – любая характеристика или элемент информационной системы, использование которых нарушителем может привести к реализации угрозы. [13]

Если есть какие-либо действия, то есть и носители этих действий, из которых эти угрозы могут исходить – ***источники угроз (ИУ).*** В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления.

Все источники угроз безопасности информации можно разделить на три основные группы:

1. Обусловленные действиями субъекта (антропогенные источники угроз).
2. Обусловленные техническими средствами (техногенные источники угрозы).
3. Обусловленные стихийными источниками.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть:

1. [A] объективными
2. [B] субъективными
3. [C] случайными.

Тема 2. ОСНОВНЫЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ.

Международные стандарты. Законы РФ, указы Президента РФ, ГОСТЫ, документы ФСТЭК в области защиты информации. Приказы МО РФ, командующего КВ, командира части по защите компьютерной информации.

Тема 3. ОСНОВНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Понятие метода защиты информации. Характеристика основных методов ЗИ. Программно-аппаратные методы ЗИ.

В соответствии с Государственным Стандартом Российской Федерации Р 50922-96 [4] под ***методом* (способом) *защиты информации*** понимают порядок и правила применения определенных принципов и средств защиты информации

основные группы методов ЗИ:

- правовые (законодательные);
- экономические;
- организационные (административные);
- инженерно-технические;
- технические;
- программно – аппаратные.

К *основным программно-аппаратным методам защиты информации* можно отнести

следующие:

- криптографические;
- стеганографические;
- эталонных характеристик.

Криптографические методы ЗИ. Основные понятия и определения. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Функции хэширования. Алгоритм ЭЦП. Реализация криптографических методов зашиты информации.

Суть ***криптографического*** метода защиты информации заключается в преобразовании открытых данных в зашифрованные при помощи шифра

Стеганографические методы ЗИ. Введение в цифровую стеганографию. Стеганографические методы защиты информации. Состав и основные принципы работы стегосистемы ЦВЗ. Области применения стеганографии.

Суть ***стеганографического*** метода защиты информации заключается в том, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимания объект, который затем открыто транспортируется адресату. При стеганографии скрывается сам факт существования тайного сообщения.

Методы эталонных характеристик. Идентификация и аутентификация пользователей. Защита программ и дистрибутивов от копирования. Регистрация и анализ событий. Методы обнаружения модификации данных.

Суть метода ***эталонных характеристик*** заключается в анализе аппаратно-программной среды и формировании её уникального идентификатора. Только субъект, обладающий этим уникальным идентификатором, будет иметь (не иметь) право доступа к информации.

Тема 4. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.

Понятие и классификация средств ЗИ. Краткая характеристика средств разграничения доступа (СРД). Вспомогательные программно-аппаратные средства.

Под средством защиты информации понимают – техническое, программное средство, вещество и/или материал, предназначенное или используемое для защиты информации.

Слайд таблица средств ЗИ

Архитектура и компоненты системы СРД Secret Net. Защитные механизмы системы Secret Net. Аппаратная поддержка системы Secret Net.

Предназначение и классификация МЭ. Схемы подключения сегментных МЭ и технология сетевой трансляции адресов. Обзор современных МЭ.

Общие сведения о компьютерных вирусах. История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса и основные этапы его жизненного цикла. Наиболее распространённые компьютерные вирусы и их классификация.

Организация антивирусной защиты. Уровни защиты от компьютерных вирусов. Общая характеристика сертифицированных антивирусных средств. Основные положения приказов Министра Обороны РФ, Командующего КВ по противодействию компьютерным вирусам.

Тема 5. МЕХАНИЗМЫ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ.

Общие сведения о реализации защиты ИПО в операционных системах. Назначение состав и основные возможности ОС МСВС. Основные задачи администратора системы (подключение пользователей, резервное копирование, мониторинг системы и др.). Особенности загрузки системы. Подключение файловых систем. Маркировка документов при печати и журнал регистрации печати, назначение службы Samba.

Состав и характеристика основных элементов «Система защиты от НСД». Контроль целостности файловой системы. Командный и графический интерфейс СЗИ ОС МСВС. Использование матрицы установления полномочий. Разграничение доступа по уровням секретности и мандатам. Комбинированные методы разграничения доступа. Особенности программной реализации контроля установленных полномочий. Программы резервного копирования.

ОС МСВС 3.0 ФЛИР.80001-01 - это мобильная, многопользовательская, многозадачная операционная система, поддерживающая симметричные многопроцессорные архитектуры и работающая как в режиме командной строки, так и в режиме графического интерфейса.

Основное назначение ОС МСВС 3.0 - управление ресурсами системы и процессами, использующими эти ресурсы при вычислениях.

ОС МСВС 3.0 - это программное изделие, поставляемое в виде загрузочного модуля и комплекта эксплуатационной документации. Загрузочный модуль поставляется на CD-ROM, а комплект эксплуатационной документации поставляется на бумажном носителе.

В состав ОС МСВС 3.0 входят четыре комплекса:

- Базовая конфигурация ОС ФЛИР.91100-01;
- Система графического интерфейса ФЛИР.91200-01;
- Система защиты от НСД ФЛИР.91300-01;
- Средства разработки ФЛИР.91400-01.

Файловая система ОС МСВС 3.0 соответствует типу **EXT2** FS, обеспечивает поддержку длинных имен, символических связей, а также обеспечивает поддержку файловых систем ISO9660, FAT (MS-DOS), NTFS (Windows NT).

В составе СЗИ ОС МСВС 3.0 функционируют следующие механизмы, обеспечивающие разграничение доступа и аудит:

1) мандатное управление доступом (Mandatory Access Control - MAC). Мандатная политика позволяет определять для информации уровни секретности и принадлежность к различным категориям;

2) дискреционное управление доступом (Discretional Access Control - DAC). Каждому файлу ОС МСВС 3.0 сопоставляется список прав доступа (Access Control List - ACL), позволяющий контролировать доступ к данному файлу с точностью до отдельного пользователя системы;

3) аудит. В ОС МСВС 3.0 функционирует система аудита, позволяющая протоколировать события отдельно для каждого пользователя системы. ОС МСВС 3.0 позволяет осуществлять аудит открытия файлов, запуска программ, установку драйверов, входа и выхода пользователей и других событий;

4) привилегии. В ОС МСВС 3.0 функционирует система привилегий (т.н. capabilities), позволяющая отдельным пользователям выполнение различных административных действий.

Тема 6. ОСНОВЫ ФОРМАЛИЗАЦИИ ПРОЦЕССОВ ЗАЩИТЫ И ОСНОВНЫЕ МАТЕМАТИЧЕСКИЕ МОДЕЛИ.

Направления формализации процессов защиты информации. Матричные и многоуровневые модели доступа.

В настоящее время наибольшее распространение получили матричные и многоуровневые модели доступа. Указанным моделям соответствуют дискретное (избирательное) и мандатное управление доступом.

Наиболее известна: **матричная модель** защиты – **Харрисона-Руззо-Ульмана**, получившую на сегодняшний день широкое распространение.

Многоуровневая модель Белла и Лападулы и *решетчатая* **модель Деннинга.**

Вопрос 2. Проблемы обеспечения информационной безопасности отечественных информационных систем.

Информация, информационные ресурсы, информационные технологии, информационное противоборство стали во многом синонимами основных направлений развития вооружения и военной техники, способов и форм применения вооруженных сил большинства стран мира. Российские Вооруженные Силы не являются в этом плане исключением. Вместе с тем, надо признать, что «информационные составляющие» в Государственной программе вооружения, Государственном оборонном заказе, представлены не достаточно.

Концепция единого информационного пространства является базовой для создания многофункциональных систем и комплексов межвидового применения, включая средства (системы) получения информации, ее обработки, управления, средства поражения. С учетом этого обстоятельства под объектами информационной инфраструктуры (ОИИ) Вооруженных Сил Российской Федерации (ВС РФ) будут пониматься объекты, предназначенные для получения (актуализации) информационных ресурсов, их обработки с целью выделения искомой информации или ее представления в требуемом виде, хранения информационных ресурсов в виде, удобном для их последующего использования, распределения информационных ресурсов между ОИИ, целевого использования информационных ресурсов для решения задач, возлагаемых на ВС РФ.

Многообразны и ОИИ Вооруженных Сил Российской Федерации, которые с достаточной степенью условности могут быть классифицированы следующим образом:

- средства и системы создания (актуализации) информационных ресурсов;
- средства и системы предварительной обработки, преобразования,
- архивирования и хранения информационных ресурсов;
- средства и системы распределения, обеспечение доступа к информационным ресурсам;
- средства и системы целевого использования информационных ресурсов.

К ОИИ, предназначенным для получения (актуализации) информационных ресурсов относятся:

- космические средства видео-, радио-, радиотехнической разведки; пилотируемые и беспилотные разведывательные авиационные комплексы;
- гидроакустические комплексы и системы освещения подводной обстановки;
- радиолокационные средства и системы наземного, морского и воздушного базирования;
- космические картографические комплексы и др.

К ОИИ, предназначенным для предварительной обработки, преобразования, архивирования и хранения информации, относятся:

- стационарные центры и мобильные системы, предназначенные для

получения цифровых карт (моделей) местности;
- стационарные и мобильные центры обработки космической разведывательной информации;
- подвижные пункты обработки данных, получаемых от пилотируемых и беспилотных средств воздушной разведки;
- центры подготовки эталонной информации для средств поражения и др.

К ОИИ, предназначенным для распределения информационных ресурсов, относятся стационарные и мобильные узлы связи ВС РФ, а также специальные системы связи ВС РФ.

К важнейшим ОИИ целевого использования информационных ресурсов, в значительной мере определяющих облик и боевые возможности Вооруженных Сил, относятся:
- автоматизированные системы управления, системы и средства ВС РФ (стратегического, оперативно-стратегического, тактического назначения);
- системы и комплексы средств поражения (надводные корабли, подводные лодки различного назначения, авиационные комплексы, ракетные комплексы и др.);
- системы и комплексы боевого обеспечения (подготовки полетных заданий, моделирования боевых действий, радиоэлектронного подавления и др.).

К самостоятельным ОИИ следует также отнести центры моделирования, используемые в интересах обучения, а также поддержки принятия решений.

Практически во всех перечисленных типах ОИИ ВС РФ используются информационные технологии, предназначенные для защиты информационных ресурсов и систем на всех этапах их целевого использования.

В ОИИ, предназначенных для создания информационных ресурсов, к таким технологиям относятся:
- сжатие данных;
- кодирование информации с борта космических и авиационных разведывательных средств;
- защита каналов управления от несанкционированного доступа.

В ОИИ, предназначенных для предварительной обработки, преобразования и хранения информационных ресурсов, типовыми технологиями являются:
- защита от несанкционированного доступа;
- разграничение полномочий пользователей;
- идентификация пользователей;
- кодирование информации;
- копирование больших массивов информации с целью обеспечения ее надежного хранения;
- контроль целостности информации и др.

В целом близкие или аналогичные технологии используются в телекоммуникационных ОИИ и ОИИ, предназначенных для целевого использования информационных ресурсов. С учетом различий в сроках создания, принципах построения, технической и технологической основы значительная часть указанных выше технологий реализована на основе различных и, как следствие, неунифицированных решений. В результате, в Вооруженных Силах применяется несколько десятков операционных систем (более 50) и еще большее количество систем управления базами данных. В сочетании с практически полным спектром аппаратных платформ данное обстоятельство обусловливает крайне низкий уровень совместимости эксплуатируемых ОИИ, сложность их общесистемной интеграции, проблемный характер многих вопросов, связанных с практической реализацией концепции единого информационного пространства Вооруженных Сил.

Вопрос 3. Построение комплексной системы информационной безопасности. Перспективы и тенденции развития.

В настоящее время на объектах ВТ КВ в основном используется следующее системное ПО: Операционная система ПИ 15Э99 (MS Windows NT v.4.0), Защищенная ОС МСВС 3.0, СУБД Oracle 8.05, SQL Server.

слайд

Основными средствами защиты информации на объектах ВТ КВ являются: СПО разграничения доступа «SecretNet», ПАК «Соболь-PCI», программы антивирусной защиты Dweb v. 4.32b. Причём данные средства защиты установлены на все ПЭВМ и сервера. Вместо «SecretNet» может устанавливаться СРД «Аккорд» и АМДЗ «Аккорд». Обновление антивирусных баз производится централизованно по мере поступления обновлений. Обеспечения целостности данных на объектах ВТ КВ обеспечивается с помощью средств разграничения доступа «SecretNet», ПАК «Соболь-PCI» и ОС МСВС 3.0. В процентном соотношении ОС МСВС 3.0. составляет около 5-10 % от MS Windows NT v.4.0.

С целью создания условий минимально необходимых для решения проблемы стандартизации и унификации программно-технических средств, удовлетворяющих требованиям технологической независимости и информационной безопасности вооружения и военной техники Вооруженных Сил, включая ОИИ, Министерством обороны Российской Федерации в течение последнего десятилетия предпринимаются целенаправленные усилия по созданию, в рамках специальных технологических программ, защищенных компьютерных технологий, которые, как представляется, станут технологической основой большинства перечисленных выше типов ОИИ, а также единого информационного пространства Вооруженных Сил. На данном этапе основные усилия сосредоточены на создании:

- базовых средств общего программного обеспечения (операционные системы, системы управления базами данных, средства разработки прикладного программного обеспечения и др.);
- отечественных базовых микропроцессоров и вычислительных средств на их основе, полностью удовлетворяющих требованиям информационной безопасности.

Разработки указанных средств, в основном, сконцентрированы в комплексных целевых программах Министерства обороны Российской Федерации, в частности, «Интеграция-СВТ», «Информатика-2016», «Оператор», «Инфобор» и программах, ориентированных на создание конкретных типов ОИИ ВС РФ, основными из которых являются связанные с созданием перспективных систем ракетно-ядерного оружия, стратегических носителей вооружения, автоматизированных систем управления войсками и оружием в стратегическом, оперативно-стратегическом, тактическом звеньях управления, боевого самолета пятого поколения и др.

Предусматривается, что с помощью защищенных компьютерных технологий, в конечном счете, применительно к ОИИ будут решены следующие задачи:

на этапе создания - стандартизация, унификация, максимальное сокращение типажа программно-вычислительных средств, средств телекоммуникаций, отображения информации, разработка типовых механизмов обеспечения безопасности информации на всех этапах жизненного цикла ОИИ;

на этапе поддержания процесса эксплуатации – мониторинг информационных угроз, проблем информационной и технической совместимости, разработка типовых механизмов оперативного реагирования с целью их устранения или минимизации последствий;

на этапе развития - расширение спектра технологий, включаемых в понятие защищенные компьютерные технологии, с целью повышения эффективности целевых задач в условиях информационных шумов (непреднамеренные воздействия) и целенаправленного информационного противодействия.

Технической основой для решения указанных задач в ближайшей перспективе являются *следующие практические результаты, полученные в ходе реализации технологических программ*:

- защищенная многоплатформенная операционная система МСВС 3.0, предназначенная для использования на ЭВМ с процессорами с архитектурами spark и Mips, а также (на переходный период) Intel;
- защищенная система управления базами данных « Линтер-ВС» 6.0 (второй уровень защищенности согласно документам Гостехкомиссии РФ);
- программные средства общего применения (обеспечение повседневной деятельности должностных лиц, распределенной гипертекстовой обработки данных, разработки приложений) и средства защиты информации;
- операционная система реального времени (ОСРВ) («Багет 2.0»);
- ряд магистрально-модульных ЭВМ серии «Багет»;
- ряд высокопроизводительных ЭВМ серии «Эльбрус-90микро»;
- ряд отечественных микропроцессоров серий «Багет», «Комдив», «Эльбрус-М».

Организационные аспекты создания и внедрения защищенных компьютерных технологий в отношении ОИИ связаны в основном со следующими моментами:

1. восстановлением на федеральном уровне программно-целевого планирования поддержания и развития систем вооружения, включая ОИИ («Основы военно-технической политики Российской Федерации на период до 2015 года и дальнейшую перспективу»), разработки исходных данных для формирования плана строительства Вооруженных Сил Российской Федерации на 2006 - 2010 годы, Государственной программы вооружения на 2006 - 2015 годы и последующий период;
2. совершенствованием на федеральном уровне системы управления ГОЗ, в частности, с созданием Госкомоборонзаказа России, обусловливающим, по-видимому, необходимость уточнения функций федеральных органов исполнительной власти, генеральных заказчиков Минобороны России по формированию и реализации ГОЗ, в отношении ВВТ Минобороны России и других силовых структур, включая ОИИ;
3. принятием на уровне Минобороны России ряда концептуальных документов, определяющих цели, порядок, задачи внедрения защищенных компьютерных технологий в ОИИ, в частности:

- 13.05.2002 г вышел приказ Министра обороны Российской Федерации № 190 от. «О принятии на снабжение ВС РФ защищенных ОС МСВС 3.0, СУБД «Линтер-ВС» 6.0 и комплекса программных средств обеспечения повседневной деятельности должностных лиц КП «Офис» 1.0».
- «Концепции создания и оснащения базовыми информационными компьютерными технологиями Вооруженных Сил Российской Федерации» (2001 г.);
- «Основных направлений технической реализации концепции развития системы управления, основанной на базовых информационных защищенных

компьютерных технологиях Вооруженных Сил Российской Федерации», утвержденные начальником Генерального штаба ВС РФ и начальником вооружения ВС РФ (2002 г.);

- указаний Министра обороны Российской Федерации от 19 августа 2002 года № 331/3/0437 «Об организации работ по КЦП «Развитие базовых информационных защищенных компьютерных технологий на период до 2016 года»;
- указаний Министра обороны Российской Федерации от 12 марта 2003 года № 331/3/317дсп «Об организации работ по созданию отечественных информационных технологий и оснащению ими Вооруженных Сил Российской Федерации»;
- выпуском совместного приказа Минобороны и Минпромнауки России (2002 г.), которым утвержден генеральный конструктор информационных технологий Вооруженных Сил Российской Федерации.

Методологические аспекты, связанные с применением защищенных компьютерных технологий в ОИИ, в основном определяются следующими моментами:

- необходимостью обоснования рационального уровня унификации (стандартизации) базовых программно-технических средств, их типажа,
- стратегии их внедрения с учетом ресурсных ограничений, специфики построения, технического состояния и других условий, определяющих
- особенности функционирования ОИИ;
- выбором приоритетов, этажности их реализации в ОИИ различных типов при переходе к единому информационному пространству Вооруженных Сил;
- совершенствованием структуры комплексных целевых программ, ориентированных на создание защищенных компьютерных технологий, повышением эффективности управления такими программами, повышением объективности комплексной оценки полученных результатов;
- необходимостью разработки в кратчайшие сроки общего подхода к построению ОИИ на основе защищенных компьютерных технологий, их интеграции в типовые боевые системы Вооруженных Сил, аналогичного Единой технической архитектуре, принятой в министерстве обороны США и предназначенной для обеспечения совместимости различных систем управления всеми видами высокотехнологического оружия;
- разработкой методов комплексной оценки систем, состоящих из большого количества ОИИ, находящихся в различных состояниях и различных режимах функционирования;
- разработкой эффективных методов (средств) верификации программной и аппаратной основы защищенных компьютерных технологий;
- совершенствованием системы сертификации защищенных компьютерных технологий.

Технологические аспекты применения защищенных компьютерных технологий в ОИИ обусловлены:

- проблемами сохранения (переноса) ранее созданного программного обеспечения;
- отсутствием современных стандартов на технологию создания
- мобильного прикладного программного обеспечения;
- отсутствием нормативной и технической документации, определяющей порядок, технологию построения единого информационного пространства Вооруженных Сил и функционирования в нем ОИИ;

- необходимостью выработки общих принципов технической интеграции в ОИИ средств, созданных на основе отечественных защищенных компьютерных технологий, и средств, создаваемых с использованием зарубежных комплектующих и программного обеспечения.

Несмотря на проблемный характер указанных моментов, следует отметить, что они во многом обусловлены недостатками организации работ в области защищенных компьютерных технологий.

При этом в качестве практической основы для решения перечисленных и ряда других технологических проблем **уже в ближайшей перспективе могут быть использованы:**

- технологии перевода локальных вычислительных сетей, функционирующих под управлением операционной системы Windows NT 4.0, на управление операционной системы МСВС;
- микропроцессоры отечественной разработки, изготовленные за рубежом по технологии 0,13…0,35 мкм, вычислительные средства на их основе;
- технологические возможности специализированного комплекса 1Х1 (завершение государственных испытаний во 2 квартале 2003г.), обеспечивающего выпуск СБИС, включая микропроцессоры, с технологическими нормами 0,35...0,5 мкм.

В частях КВ перевод автоматизированных систем на защищенные программные средства предлагается проводить в 3 этапа:

Слайд

1. Установка в системе файлового сервера, сервера БД с СУБД и сервера ГОД под ОС МС ВС.
   - Установка в системе СЗИ, в т.ч. рабочих мест администраторов сети, ОБИ, БД, генерации паролей, станций печати.
   - Установка в системе сервера приложений и средств терминального сервиса.
   - Перевод СПО на функционирование в режиме терминального сервиса с переносом данных в среду ОС МС ВС.
   - Установка на рабочих местах должностных лиц ОС МС ВС и средств терминального сервиса.

На первом этапе обеспечивается:

- функционирование автоматизированной системы с СЗИ и хранением основной части данных в защищенной среде ОС МС ВС;
- функционирование гетерогенной ЛВС и имеющегося СПО в режиме терминального сервиса.

2. - Перевод СПО (в первую очередь серверных компонентов) под ОС МС ВС с использованием в основном средств гипертекстовой обработки данных и СУБД

- Переход на использование офисных средств под ОС МС ВС (текстового редактора, электронной таблицы и т.п.).

На втором этапе обеспечивается:

- совместное функционирование защищенного и имеющегося СПО в гетерогенной ЛВС;
- возможность разработки нового и перевода имеющегося СПО в защищенную среду.

3. Окончательный перевод СПО под ОС МС ВС 3.0.

- В режиме терминального сервиса функционируют покупные программные средства информационно-справочного характера (средства распознавания текстов,

справочные информационные системы «Консультант Плюс», «Гарант», бухгалтерия «1С» и т.п.

•На третьем этапе обеспечивается:

функционирование автоматизированной системы в штатном защищенном режиме с обеспечением возможности обработки грифованной информации и ввода системы в эксплуатацию

Таким образом, сегодня на занятии мы:

1. **закрепили ранее полученные по дисциплине,**
2. **ознакомились с перспективами и тенденциями развития защиты информации в Космических войсках.**

В настоящее время в России имеются технологическая основа, комплексные целевые технологические программы, ориентированные на создание защищенных компьютерных технологий, обеспечивающих, в основном, создание, поддержание, развитие технологически независимых и информационно безопасных объектов информационной инфраструктуры Вооруженных Сил Российской Федерации.

Старший преподаватель 27 кафедры к.т.н.
подполковник С.Краснов