Тема 1.1. Предмет и задачи программно-аппаратной защиты информации

Раздел 1. Основные принципы программной и программно-аппаратной защиты информации

Преподаватель: Попов Никита Вячеславович.

Введение

Широкое использование компьютерных информационных технологий во всех сферах жизни современного общества делает вполне закономерной и весьма актуальной проблему компьютерной защиты информации, или иначе, проблему обеспечения информационной безопасности. В условиях интенсивного развития рынка информационных продуктов и услуг информация становится полноценным товаром, обладающим своими стоимостными характеристиками и потребительскими свойствами. Подобно любым другим традиционно существующим товарам, информация также нуждается в своей сохранности и, следовательно, надежной защите.

Предмет и задачи программно-аппаратной защиты информации

В методологии анализа информационной безопасности обычно выделяют следующие основные понятия:

- объект информационной безопасности;
- существующие и потенциально возможные угрозы данному объекту;
- обеспечение информационной безопасности объекта от проявления таких угроз.

Если объектом информационной безопасности выступает сама информация, то для нее наиболее важным является сохранение таких свойств, как:

- целостность;
- конфиденциальность;
- +доступность.

Предмет и задачи программно-аппаратной защиты информации

Целостность информации заключается в ее существовании в неискаженном виде по отношению некоторому фиксированному СОСТОЯНИЮ.

Конфиденциальность – это свойство, указывающее на необходимость введения Ограничений доступа к данной информации для определенного круга лиц.

доступность информации — это ее свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации.

Весьма распространенным и вполне естественным является также рассмотрение безопасности информации в инфраструктуре конкретной информационной системы (ИС). Такие системы представляют собой Взаимосвязанную совокупность средств, методов и персонала, обеспечивающих сбор, хранение, обработку, передачу и отображение информации в интересах достижения поставленной цели. Целью создания ИС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (в случае необходимости). Информация является при этом конечным «продуктом потребления» и выступает в качестве центральной компоненты информационной системы. Объектом информационной безопасности становится в этом случае данная информационная система.

Предмет и задачи программно-аппаратной защиты информации

В методологическом плане общим основанием для отнесения данного объекта к множеству объектов информационной безопасности является наличие в нем так называемого «информационного измерения» и необходимость обеспечения безопасности этого «измерения». К «информационно измеряемым» объектам относятся объекты, для которых одной из важных структурных составляющих является либо сама информация, либо деятельность, предметом которой она является.

С этой точки зрения, упомянутые ранее информационные системы, безусловно, являются объектами информационной безопасности. В инфраструктуре таких систем не только представлена различная информация, но и реализуются процессы, связанные с ее преобразованием.

Предмет и задачи программно-аппаратной защиты информации

Учитывая системный характер влияния на компьютерную информационную безопасность многочисленных факторов и обстоятельств, вполне очевидно, что эффективное решение этой проблемы возможно только на основе комплексного и целенаправленного использования всех имеющихся средств, обеспечивающих в целом необходимый и, главное, гарантированный уровень защищенности информационных ресурсов.

Следует отметить, что рассматриваемая проблема обеспечения информационной безопасности весьма актуальна для нашей страны. Нельзя считать, что из-за унаследованной информационной замкнутости, некоторой технической отсталости Россия мене уязвима в информационном отношении, чем другие страны. Скорее наоборот: достаточно высокая степень централизации структур государственного управления российской экономикой может привести к гибельным последствиям в результате информационной агрессии.

В 2000 году Президентом была утверждена Доктрина информационной безопасности Российской Федерации, устанавливающая официальную систему взглядов на содержание национальных интересов России в информационной сфере, методы противодействия существующим угрозам и систему обеспечения информационной безопасности. При этом были учтены проблемы развития российского общества, порожденные как советским периодом его истории, так и периодом продолжающихся социально-экономических и политических преобразований.

Предмет и задачи программно-аппаратной защиты информации

Так, с 1992 года выявление угроз информационной безопасности и подготовка предложений по противодействию этим угрозам возложено законодательством на Совет Безопасности РФ, при котором образована Межведомственная комиссия по информационной безопасности. С 1996 года в Комитете Государственной Думы РФ существует подкомитет по информационной безопасности, а также экспертный совет по законодательству в области обеспечения информационной безопасности. Большую работу в этой области выполняют также федеральные органы исполнительной власти, а также государственные органы субъектов РФ.

Интенсифицируются исследования проблем обеспечения программно-аппаратной компьютерной информационной безопасности, выполняемые как в естественных и технических науках, так и в рамках гуманитарных наук. Комплексное научное осмысление этих проблем существенно способствует развитию индустрии средств защиты информации, используемых, в том числе, в современных компьютерных и телекоммуникационных системах.

Развивается правовое регулирование отношении в области обеспечения информационной безопасности. Приняты такие базовые законодательные акты как законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О связи», «О государственной тайне», первая и вторая части Гражданского кодекса РФ, новые редакции Уголовного и Уголовно-процессуального кодексов РФ, ряд законов, регулирующих отношения в области средств массовой информации, и др.

Аппаратные средства защиты информации

Аппаратные средства – это технические средства, используемые для обработки данных.
Сюда относятся:

- персональный компьютер (комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач).
- периферийное оборудование (комплекс внешних устройств ЭВМ, не
- находящихся под непосредственным управлением центрального процессора).
- физические носители машинной информации.

Аппаратные средства защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

1. Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
2. Генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;
3. Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
4. Специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;
5. Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
6. Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

Программные средства обеспечения защиты информации

Программные средства - это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения. К ним относятся:

- Программное обеспечение (совокупность управляющих и обрабатывающих программ). Состав:
- Системные программы (операционные системы, программы технического обслуживания);
- Прикладные программы (программы, которые предназначены для решения задач определенного типа, например редакторы текстов, антивирусные программы, СУБД и т.п.);
- Инструментальные программы (системы программирования, состоящие из языков программирования: C++, C#, GO и т.д. и трансляторов – комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды);
- Машинная информация владельца, собственника, пользователя.

Программные средства обеспечения защиты информации

К программным средствам защиты относятся специальные программы, которые предназначены для выполнения функций защиты и включаются в состав программного обеспечения систем обработки данных. Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п. По функциональному назначению их можно разделить на следующие группы:

1. Идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей;
2. Определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей;
3. Контроль работы технических средств и пользователей;
4. Регистрация работы технических средств и пользователей при обработки
5. Информации ограниченного использования;
6. Уничтожения информации в ЗУ после использования;
7. Сигнализации при несанкционированных действиях;
8. Вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

Задачи обеспечения программно-аппаратной защиты информации

Под программно-аппаратным обеспечением средств защиты операционной системы традиционно понимается совокупность средств и методов, используемых для решения следующих задач:

1. Управление оперативной и виртуальной памятью компьютера;
2. Распределение процессорного времени между задачами в многозадачной операционной системе;
3. Синхронизация выполнения параллельных задач в многозадачной операционной системе;
4. Обеспечение совместного доступа задач к ресурсам операционной системы.

Задачи обеспечения программно-аппаратной защиты информации

Основные выводы о способах использования средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.
2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.
3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.
4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

Классификация методов и средств программно-аппаратной защиты информации

Технические средства. Это различные по типу устройства, которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны - недостаточная гибкость, относительно большие объём и масса, высокая стоимость.

При защите информационных систем этот элемент имеет весьма важное значение, хотя стоимость средств технической защиты и охраны велика. Инженерно-технический элемент системы защиты включает в себя:

1. Сооружения физической защиты от проникновения посторонних лиц на территорию, в здание и помещения;
2. Средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализации, информирования и идентификации);
3. Средства противопожарной охраны;
4. Технические средства контроля, предотвращающие вынос персоналом из помещений специально маркированных предметов, документов, дискет, книг.

Классификация методов и средств программно-аппаратной защиты информации

Программно-аппаратная защита информации. Программные средства включают программы для идентификации пользователей, контроля доступа, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки - ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Программно-аппаратный элемент системы защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно-технической и организационной защите. Элемент включает в себя:

1. Автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;
2. Программы защиты информации, работающие в комплексе с программами обработки информации;
3. Программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных).