Основные принципы защиты информации в компьютерных системах.

Антонова И.М.
гр. И-411

Под информацией, применительно к задаче ее защиты понимается сведения о лицах, предметах, фактах, событиях явлениях и процессах независимо от формы их представления.

К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, выдвигаемыми собственником информации.

Любая компьютерная система (КС) использует стандартное и специализированное оборудование и программное обеспечение, выполняющее определенный набор функций по обработке информации. В их состав, как правило, включают функции:

- *ограничения и разграничения доступа к информации,*
- *обработки информации,*
- *обеспечения целостности информации,*
- *защиты информации от уничтожения,*
- *шифрования и электронной цифровой подписи, операционной системы, BIOS и другие.*

Целостность информации и защита, ограничение доступа к ней обеспечивается специализированными компонентами системы, использующими криптографические методы защиты. Для того, чтобы компьютерной системе можно было полностью доверять, ее необходимо аттестовать:

- *определить множество выполняемых функций,*
- *доказать конечность этого множества,*
- *определить свойства всех функций.*

Любая система защиты строится на известных разработчику возможностях операционных систем (ОС), причем для построения надежной компьютерной системы требуются полные знания всех возможностей ОС. В настоящее время отечественные разработчики располагают полными знаниями только об одной операционной системе — DOS. Таким образом, к полностью контролируемым системам можно отнести КС, работающие под операционной системой DOS, или КС собственной разработки.

При использовании системы ее функциональность не должна нарушаться, иными словами, необходимо обеспечить:

- *целостность системы в момент ее запуска;*
- *целостность системы в процессе функционирования.*

Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, чтобы изменить ПО, необходимо получить доступ к соответствующей плате и заменить микросхему.

Основным аппаратным элементом системы является серийно выпускаемая аттестованная плата КРИПТОН-4 с помощью которой проверяется целостность системы и выполняется шифрование по ГОСТ 28147-89. Система предполагает наличие Администратора безопасности, который определяет взаимодействие между управляемыми ресурсами: пользователями, программами, логическими дисками, файлами (дискреционный и мандатный доступ), принтером, дисководами.

Диски можно разделить по пользователям и/или по уровню секретности размещаемой на них информации. Сначала администратор устанавливает уровень секретности диска, а затем определяет круг лиц, имеющих доступ к этому диску. По форме хранения информации диски подразделяются на открытые и шифруемые; по уровню доступа:

- *доступные для чтения и записи,*
- *доступные только для чтения,*
- *недоступные (заблокированные).*

Руководящие документы государственной технической комиссии России.

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации разработала и опубликовала пять руководящих документов, посвященных вопросам защиты информации в автоматизированных системах ее обработки. Основой этих документов является концепция защиты средств вычислительной техники (СВТ) и АС от несанкционированного доступа к информации, содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков данных документов, основная задача средств безопасности - это обеспечение защиты от несанкционированного доступа к информации.

В руководящих документах ГТК представлены семь принципов защиты информации:

1. *защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации;*

2. *защита СВТ обеспечивается комплексом программно-технических средств;*

3. *защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер;.*

4. *защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;*

5. *программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС);*

6. *неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты;*

7. *защита АС должна предусматривать контроль эффективности средств защиты от НСД, который либо может быть периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.*

В используемых в настоящее время аппаратно-программных системах защиты от НСД для частично контролируемых систем серьезно рассматривать можно только функции доступа на персональный компьютер, выполняемые до загрузки операционной системы, и аппаратные функции блокировки портов ПК. Таким образом, остается большое поле деятельности по разработке модулей безопасности для защиты выбранных процессов в частично контролируемых системах.

Спасибо за внимание!