Лабораторная работа №10

Тема «Исследование реализации системы защиты программными средствами»

ВЫПОЛНИЛ

Олишкевич Игорь Русланович

Группа 25-ПО

Задание: изучить методы реализации систем защиты программными средствами.

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Система защиты информации создается для объекта информатизации. Цель создания системы — обеспечение целостности, доступности и конфиденциальности обрабатываемой на объекте информации.

Классификация:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. 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:
   1. специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
   2. устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
   3. схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных;
   4. устройства для шифрования информации (криптографические методы);
   5. модули доверенной загрузки компьютера.
2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, 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](http://cyclowiki.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80&action=edit&redlink=1) и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств):
   1. Встроенные средства защиты информации;
   2. [Антивирусная программа](http://cyclowiki.org/w/index.php?title=%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0&action=edit&redlink=1) (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом;
   3. Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и [криптографических](http://cyclowiki.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) систем, существует много других доступных внешних средств защиты информации;
   4. [Межсетевые экраны](http://cyclowiki.org/w/index.php?title=%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD&action=edit&redlink=1). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой;
   5. VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.
3. Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства;
4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении;
5. По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

Анализ объекта защиты:

1. Определение границ объекта защиты и обследование его среды:
   1. определение ресурсов среды, используемых для размещения, функционирования и эксплуатации объекта защиты;
   2. анализ зависимости безопасности объекта защиты от среды его функционирования и эксплуатации.
2. Обследование объекта защиты:
   1. анализ и классификация обрабатываемой информации, разделение ее по категориям доступа;
   2. анализ организационной структуры объекта защиты, порядка его функционирования и эксплуатации;
   3. анализ функциональной структуры объекта защиты, состава программного обеспечения и баз данных, их функционального назначения и порядка функционирования, анализ информационных потоков;
   4. определение типового класса объекта защиты в соответствии с действующими нормативными правовыми актами.
3. Определение потенциальных угроз для объекта защиты и анализ возможных последствий их осуществления (потенциального ущерба).

Проектирование и реализация системы защиты информации:

1. Разработка частного технического задания на систему защиты информации (при необходимости);
2. Разработка организационной и функциональной структуры системы защиты информации;
3. Разработка политики безопасности и необходимых организационных документов по обеспечению безопасности объекта защиты;
4. Разработка задания по безопасности объекта защиты;
5. Разработка проектной документации на систему защиты информации;
6. Реализация системы защиты информации на объекте защиты и в его среде.

Ввод в действие системы защиты информации:

1. Разработка программы и методики испытаний объекта защиты на соответствие требованиям безопасности;
2. Проведение испытаний системы защиты информации;
3. Доработка системы защиты информации по результатам испытаний и ввод ее в опытную эксплуатацию;
4. Доработка системы защиты информации по результатам опытной эксплуатации и внесение необходимых изменений в документацию;
5. Оценка задания по безопасности;
6. Проведение приемо-сдаточных испытаний системы защиты информации.