Лабораторная работа № 17 исследование и системная классификация средств защиты информации

**Цель и содержание:**провести исследование и системную классификацию средств защиты информации

**Теоретическое обоснование**

Для решения любой задачи в АСОД в ней, как известно, должны быть предусмотрены адекватные по содержанию и достаточные по коли­честву средства, характер которых определяется также степенью форма­лизации задачи. При этом сколько-нибудь регулярной (а тем более фор­мализованной) методологии выбора необходимых и достаточных, средств для решения заданной совокупности задач не существует, такой выбор обычно осуществляется на основе непосредственного анализа конкретных задач, причем главным образом используется опыт решения аналогичных задач.

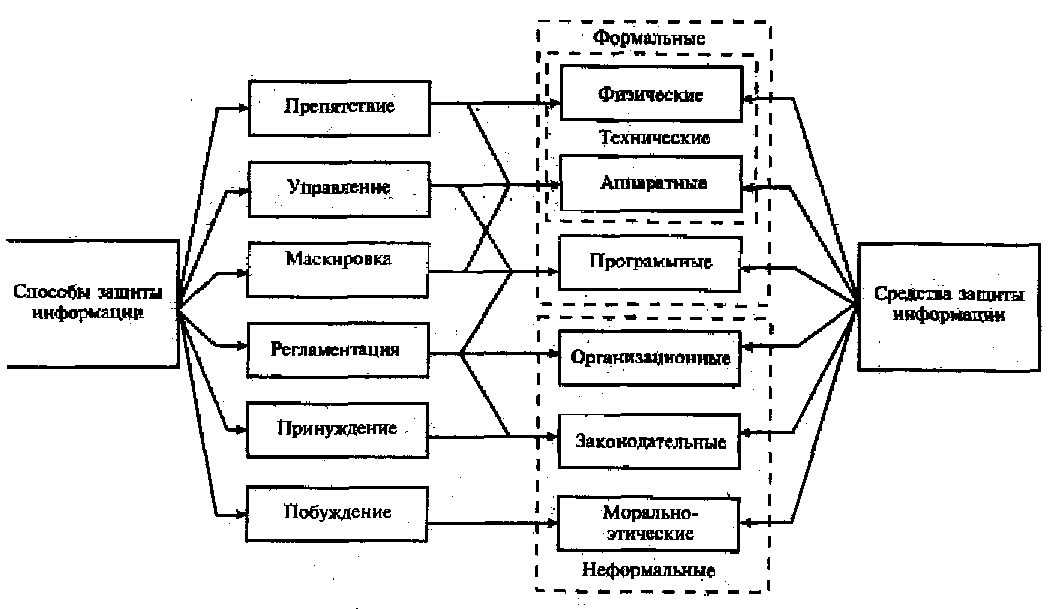
Подобным приемом воспользуемся и здесь при обосновании соста­ва необходимых средств для решения задач зашиты информации в АСОД.

К настоящему времени разработан весьма представительный по номенклатуре арсенал различных средств защиты информации, с по­мощью которых может быть обеспечен требуемый уровень защищен­ности информации в АСОД, Множество и разнообразие возможных средств защиты определяется, прежде всего способами воздействия на дестабилизирующие факторы или порождающие их причины, причем воздействия в направлении, способствующем повышению значений пока­зателей защищенности или (по крайней мере) сохранению прежних (ранее достигнутых их значений. Эти способы могут быть классифицированы так, как показано на рисунке 1.

Существо выделенных на рисунке 1 способов защиты в общих чертах может быть охарактеризовано следующий образом:

1. Препятствие заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры. Типичными примерами препятствий являются блокировки, не позво­ляющие техническому устройству или программе выйти за опасные гра­ницы; создание физических препятствии на пути злоумышленников и т.п.

2. Управление есть определение на каждом шаге функционирования АСОД таких управляющих воздействий на элементы системы, следствием которых будет решение (или способствование решению) одной или нескольких задач защиты информации.

Рисунок 1*–*Классификация способов и средств защиты информации

3. Маскировка (защищаемой информации) предполагает такие ее преобразования, вследствие которых она становится недоступной для злоумышленников или доступ к ней существенно затрудняется,

4. Регламентация, как способ запилы информации, заключается в разработке и реализации в процессе функционирования АСОД комплек­сов мероприятий, создающих такие условия обработки информации, при которых существенно затрудняется проявление и воздействие дестабили­зирующих факторов.

5. Принуждение есть такой способ защиты, при котором пользова­тели и персонал АСОД вынуждены соблюдать правила и условия обра­ботки под угрозой материальной, административной дли уголовной от­ветственности,

6. Побуждение есть способ защиты информации, при котором пользователи и персонал АСОД внутренне (т. е. материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации.

Рассмотренные способы обеспечения защиты информации реали­зуются в АСОД применением различных средств, причем различают формальные и неформальные средства. К формальным относятся такие средства, которые выполняют свои функции по защите информации формально, т. е. преимущественно без участия человека; к неформальным относятся средства, основу содержания которых составляет целенаправленная деятельность людей. Формальные средства делятся на технические (физические и аппаратные) и программные, неформальные - на организа­ционные, законодательные и морально-этические.

Выделенные на рисунке 1 классы средств могут быть определены следующим образом:

*Физические средства –*механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и си­лены, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

*Аппаратные средства -*различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру си­стемы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.

*Программные средства –*специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения АСОД с целью решения задач защиты информации.

*Организационные средства –*организационно-технические мероприятия, специально предусматриваемые в технологии функционирования АСОД с целью решения задач защиты информации.

*Законодательные средства –*нормативно-правовые акты, с по­мощью которых регламентируются права и обязанности, а также устана­вливается ответственность всех лиц и подразделений, имеющих отноше­ние к функционированию системы, за нарушение правил обработки ин­формации, следствием чего может быть нарушение ее защищенности.

*Морально-этические средства –*сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение кото­рых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

Законодательные средства формируются путем издания соответствующих юридических актов, что является прерогативой соответствую­щих органов управления. Морально-этические нормы формируются в Процессе жизнедеятельности общества. Поэтому здесь сосредоточено внимание на технических, программных и организационных средствах, являющихся основным инструментом органов защиты информации.

Общая характеристика выделенных классов средств приведена в таблице 1.

Для формирования возможно более полного арсенала потенциаль­но возможных средств защиты необходимо осуществить системный ана­лиз возможностей решения различных задач защиты средствами различ­ных классов. Существо и содержание такого анализа на уровне классов задач приведены в таблице 2, в которой даны перечни потенциально воз­можных средств защиты, которые могут быть использованы дня решения задач различных классов.

Представленные в таблице данные не претендуют на исчерпы­вающую полноту, однако они дают представление о том, что потенци­ально имеются весьма широкие возможности для создания представи­тельного арсенала средств защиты. Однако следует отдавать себе отчет, что создание и развитие необходимого арсенала средств защиты сопря­жено с большими затратами сил и средств, эти затраты, очевидно, соста­вят наибольшую долю общих расходов на защиту. Этим предопределяется необходимость особо плательного подхода к системному анализу средств защиты. Чтобы наиболее полно учесть данное обстоятельство, на рисунке 2 приведена общесистемная классификация средств, причем в ка­честве критериев классификации выбраны: класс решаемых задач защи­ты, класс средств и функциональное назначение средств. Первые два кри­терия являются очевидными, они естественным образом вытекают из предыдущего анализа. Поясним только мотивы выделения в самостоятельный класс криптографических средств. Основные из этих мотивов со­стоят в следующем:

1) криптографическое преобразование является сугубо специфическим средством защиты, причем требующим весьма тщательного отношения, поскольку видимость закрытия еще не означает действенного закрытия, а усложнение способа преобразования, естественна, ведет к увеличению расходов средств на само преобразование;

2) в условиях расширения сферы защиты информации, распространения развиваемых здесь концепций на защиту промышленной, коммер­ческой, банковской тайны, а также на защиту конфиденциальной инфор­мации существенно возрастает интерес к криптографии как средству за­щиты, поскольку небольшие объемы информации, содержащей перечисленные выше разновидности тайны, на не очень большой период времени могут быть достаточно надежно закрыты сравнительно простыми спосо­бами преобразования;

3) криптографическое преобразование данных в современных АСОД может быть реализовано как аппаратными средствами, так и про­граммными и организационными, в силу чего криптографические сред­ства не представляется возможным включить в какой-либо один из основных классов средств защиты.

Таблица1 – Общая характеристика классов средств защиты

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | Классы средств защиты | | |
| Технические | Программные | Организационные |
| 1. Основная сущность | Технические устройства, сооружения и системы, способные самостоя­тельно или в комплексе с другими средствами решать задачи системы защиты | Специальные программы, включаемые в состав программного обеспечения АСОД для решения в них (самостоятельно или в ком­плексе с другими средствами) задач зашиты | Организационно-технические  и организационно-правовые мероприятия и акты, осуществляемые в процессе проектирования, соз­дания и эксплуатации АСОД с целью решения (или обеспечения решения) задач защиты |
| 2. Достоинства | 1.Надежность функционирования  2.Независимость от субъективных факторов  3.Высокая устойчивость от модификаций | 1. Универсальность  2. Гибкость  3.Надежность функциони­рования  4.Простота реализации  5. Широкие возможности модификации и развития | 1. Широкий круг решаемых задач  2. Простоту реализации  3.Гибкость реагирования на несанкционированные действия  4. Практически неограниченные возможности изменении и разви­тия |
| 3. Недостатки | 1.Недостаточная гибкость  2.Громоздкость физиче­ских средств  3. Высокая стоимость | 1. Снижение функциональ­ных возможностей АСОД 2. Необходимость использо­вания ЗУ АСОД  3. Подверженность случай­ным или закономерным модификациям  4.Ориентация на вполне определенные типы ЭВМ | 1. Необходимость использований людей  2. Повышенная зависимости субъективных факторов  3. Высокая зависимость от общей организации робот на объекте |

Таблица 2 – Потенциально возможные средства решения задач защиты информации

|  |  |  |  |
| --- | --- | --- | --- |
| Класс задач защиты | Потенциально возможные средства решения | | |
| Технические | Программные | Организационные |
| 1. Введение избыточности элементов системы | 1. Установка дополнительных средств генерирования информации  2. Установка дополнительной аппаратуры связи  3. Выделение дополнительных каналов связи  4. Установка дополнительной аппаратуры подготовки данных.  5. Установка дополнительных устройств ввода данных  6. Установка дополнительных процессоров  7. Установка дополнительных ВЗУ  8. Установка дополнительных терминальных устройств  9. Установка  дополнительных средств выдачи данных  10. Создание дополнительного запаса сменных носителей информации  11 . Создание дополнительных ЗИП  12. Установка дополнительной контрольной и другой обеспечивающей аппаратуры  13. Создание дополнительных систем охраны и наблюдения | 1. Создание дополнительных копий:  компонентов общего программного обеспечения, компонентов системного программного обеспечения, СУБД, пакетов прикладных программ, сервисных программ  2. Разработка запасных программ наиболее важных процедур обработки данных  3. Разработка программ организации повторения процедур обработки  4. Разработка программ обеспечения процессов обработки | 1.Введение дополнительной численности: пользователей наиболее ответственных категорий, диспетчеров и операторов систем обработки, администрации банков данных, системных программистов, инженерно-технического персонала  2. Разработка дополнительных (запасных) процедур и технологических маршрутов основной обработки информации  3. Разработка дополнительных процедур и схем обеспечения обработки информации |
| 2. Резервирование элементов системы | 1.Выведшие в холодный резерв: средств генерирования информации, аппаратуры связи, каналов связи, аппаратуры подготовки данных, устройств ввода данных, процессоров, ВЗУ, терминальных устройств, контрольной и другой обеспечивающей аппаратуры, систем  (устройств) охраны, наблюдения, регулирования и т.п.  2. Выведение в горячий резерв технических средств, перечисленных в 1  3. Разработка технические средств включения в работу резервного устройства | 1. Создание копий программных элементов, находящихся в холодном резерве (на носителях, находящихся в хранилищах): базового программного обеспечения, системного программного обеспечения, прикладного программного обеспечения, специальных программ, вспомогательных программ  2. Создание копий программных элементов, находящихся в горячем резерве (на носителях, установленных на включенных устройствах. ВЗУ) — тех же компонентов, что и в п. 1  3. Разработка программ включения в работу резервных программ  4. Разработка программ включения в работу резервных технических устройств | 1 . Выведение в горячий резерв специалистов, участвующих в обработке информации: пользователей, участвующих в решении наиболее важных задач, диспетчеров, операторов системы обработки, администраторов банков данных, специалистов по защите информации, инженерно-технического и  обслуживающего персонала  2. Создание и обучение холодного резерва основных категорий специалистов  3. Разработка технологии включения в работу резервных технических средств  4. Разработка технологии включения в работу резервных программных компонентов  5. Разработка правил использования должностных лиц, находящихся в горячем резерве  6. Разработка правил использования людей, находящихся в холодном резерве |
| 3. Регулирование доступа к элементам системы | 1 . Ограждение территории  2. Установка замков на дверях помещений: простых, кодовых, программно-управляемых  3. Оборудование пультов управления техническими  средствами АСОД  индивидуальными ключами  4. Оборудование замками  устройства управления ВЗУ  5. Оснащение дверей помещений и устройств АСОД радиоуправляемыми заиками  6. Установка средств опознавания человека: по голосу, по отпечаткам пальцев, по длине и форме пальцев, по подписи, по фотокарточке, по специальной идентифицирующей карте  7. Оснащение АСОД микропроцессорными устройствами опознавания | 1. Программы поддержки программно-управляемых замков  2. Программы поддержки автоматизированных контрольно-пропускных пунктов  3. Программы опознавания: по паролю простому, по набору, по разовому  4. Программы диалоговой процедуры опознавания  5. Программы проверки прав на доступ к ресурсам АСОД | 1.Разработка и внедрение системы доступа к элементам АСОД  2. Разработка и внедрение системы идентификации людей и элементов АСОД  3.Разработка и внедрение  системы правил распределения идентифицирующей информации  4. Разработка и внедрение системы правил опознавания людей и элементов АСОД  5. Оборудование и организация работы контрольно-пропускных пунктов |
| 4. Регулирование использования элементов системы | 1 . Оснащение АСОД вычислительными машинами, имеющими в своем составе специальные регистры граничных адресов ЗУ | 1. Программы разграничения доступа к техническим средствам; по устройствам, подиям недели, по календарным датам, по часам суток  2. Программы разграничения доступа к программам:  по именам,  по функциям,  по временным параметрам (дни, даты,часы)  3. Программы разграничения доступа к  данным:  по спискам,  по матрице полномочий,  по мандату  4. Программная реализация мандатной архитектуры ЗУ | 1. Разработка и внедрение системы разграничения доступа: к техническим средствам, к элементам математического обеспечения, к программам, к массивам (базам) данных  2. Разработка и реализация мероприятий  организационного разграничения доступа |
|  |
| 5. Защитное преобразование данных | 1.Аппаратура считывания кодов  2. Аппаратура сравнения кодов  3. Аппаратура кодирования-декодирования данных  4. Аппаратура шифрования-дешифрования данных  5. Аппаратура снятия идентифицирующих данных человека  6. Аппаратура генерирования маскирующих излучений | 1 . Программы кодирования-декодирования данных  2. Программы шифрования-дешифрования данных  3. Программы расчета контрольных значений обрабатываемой информации  4. Программы сжатия-расширения данных  5. Фоновые программы для маскировки излучений рабочих программ | 1. Разработка и внедрение правил использования средств защитных преобразований данных  2. Разработка и внедрение правил генерирования, распределения и использования ключей преобразования  3. Ручное (внемашинное) преобразование данных  4. Использование жгутовых кабелей с выделением жил, генерирующих маскирующее излучение |
| 6.Контроль элементов системы | 1 Аппаратура и системы сбора, обработки и  отображения данных о текущем состоянии элементовАСОД  2. Аппаратура и системы контроля работоспособности элементов АСОД  3. Аппаратура контроля правильности функционирований технических средств АСОД: по четности, методами специального кодирования, методами повторного выполнения операций, методами параллельного выполнения операций  4. Аппаратура измерение параметров внешней среды | 1. Программы тестовой проверки состояния  аппаратуры АСОД  2. Программы контроля состояния компонентов программного обеспечения  3. То же носителей информации  4. То же элементов баз данных, (массивов информации)  5. Программы динамического контроля работоспособности элементов АСОД  6. Программы профилактического контроля работоспособности элементов АСОД  7. Программы контроля правильности функционирования АСОД: методами решения контрольных (эталонных) задач, методами контрольных точек, методами повторения процедур обработки данных, методами расчета, сопровождающих данных | 1. Разработка и внедрение правил и технологии  контроля состояния элементов АСОД  2. Разработка и внедрение правил и технологии контроля работоспособности элементов АСОД  3. Визуальные методы контроля: генерирования данных, передачи данных, подготовки машинных носителей, ввода данных, контрольных распечаток выданных данных  4. Разработка и внедрение правил и технологии контроля правильности функционирования элементов АСОД  5. Организационное наблюдение за внешней средой |
| 7. Регистрация сведений | 1. Регистраторы состояния средств обработки данных 2. То же средств системы зашиты информации  3.То же параметров внешней среды | 1. Программы регистрации каталогизации) элементов системы  2. То же элементов технологии обработки информации  3. Программы регистрации запросов  4. Программы регистрации использования элементов системы в процессе обработки информации  5. Программы регистрации проявлений дестабилизирующих факторов  6. Программы регистрации данных о нарушении зашиты информации | 1. Система правил регистрации данных, относящихся к защите информации  2. Ручное ведение регистрационных журналов |
| 8. Уничтожение информации | 1.Аппаратура уничтожения информации в ОЗУ  2. То же на регистрах  3.Тоже в ВЗУ  4. Устройства и системы уничтожения бумажных носителей  5 .То же магнитных носителей  6. Экраны, препятствующие распространению излучений  7. Фильтры, поглощающие наводки  8. Заземление аппаратуры | 1. Программы уничтожения информации в ОЗУ  2. То же на регистрах  3.Тоже в ВЗУ | 1. Разработка и внедрение организационных мер уничтожений информации (измельчение носителей, сжигание носителей)  2. Разработка и внедрение правил уничтожения информации и носителей  3.Разработка и внедрение  технологии уничтожения информации и носителей  технологии уничтожения информации и носителей |
| 9. Сигнализация | 1. Технические устройства звуковой сигнализации:  2. То же световой сигнализации  3. То же наглядного отображения | 1.Программы генерирования звуковых  сигналов  2. То же световых сигналов  3. То же сигналов наглядного отображения | 1. Подача звуковых сигналов и команд людьми  2. Включение средств звуковой или световой сигнализации  3.Разработка и внедрение системы правил подачи сигналов |
| 10. Реагирование | 1. Схемы выключения (отключений) устройств при нарушении правил защиты  2. Устройства блокирования входа-выхода при попытках несанкционированного проникновения на территорию (в помещение) | 1. Программы выключения (отключения) устройств при нарушении правил защиты  2. Программы обеспечения работы устройств (систем) блокирования входа-выхода  3. Программы псевдоработы с нарушителями | 1.Разработка и внедрение системы правил реагирования на нарушение правил зашиты  2.Разработка и внедрение мер пресечения злоумышленных действий нарушителей  3.Разработка и внедрение мер по задержанию нарушителей |

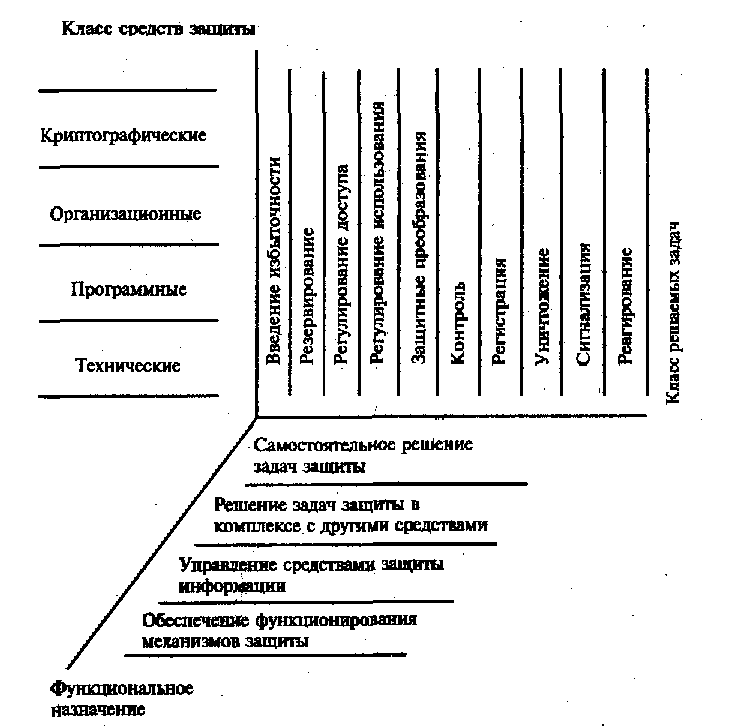


Рисунок 2 – Общесистемная классификация средств защиты информации

Перечисленными и некоторыми другими менее значивший обстоятельствами предопределено решение о самостоятельном и достаточно де­тальном рассмотрении криптографических средств.

В качестве третьего критерия классификации выбрано функцио­нальное назначение средств. Это предопределено тем, что средства защи­ты в общем случае могут использоваться как для непосредственного ре­шения задач защиты (самостоятельно или в комплексе с другими сред­ствами), так и для управления средствами защиты и для обеспечения функционирования механизмов и систем защиты.

Таким образом, в итоге общесистемной классификации средств за­щиты сформировано 160 (10x4x4) различных подклассов средств защиты.

В рамках этой классификационной структуры в следующих пара­графах самостоятельно рассматривается каждый из выделенных классов средств.

**Аппаратура и материалы:**

1. ПЭВМ

**Методика и порядок выполнения работы**

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях
2. Изучить классификацию способов и средств защиты информации
3. Ознакомиться с перечнем потенциально возможных средств решения задач защиты информации
4. Оформить отчет

**Содержание отчета и его форма**

Отчет должен иметь форму согласно оформлению простого реферата. Титульный лист должен включать название дисциплины, название лабораторной работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть лабораторной работы должна содержать:

1. Классификацию способов и средств защиты информации
2. Общую характеристику классов средств защиты
3. Потенциально возможные средства решения задач защиты информации
4. Общесистемную классификацию средств защиты информации
5. Выводы по проделанной работе

**Вопросы для защиты работы**

1. Приведите и обоснуйте системную классификацию средств защиты информации
2. Приведите примеры потенциально возможных средств, применяемых для решения задач защиты информации