МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по лабораторным работам
по дисциплине «Основы построения и системного анализа комплексных систем обеспечения информационной безопасности»
для студентов
Специальности 10.05.03 Информационная безопасность автоматизированныхсистем
Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Оглавление

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Основы построения и системного анализа комплексных систем обеспечения информационной безопасности» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» фундаментальных знаний и навыков системного подхода к проектированию, анализу и управлению комплексными системами информационной безопасности. В ходе освоения дисциплины студенты научатся применять методы системного анализа для выявления и оценки угроз, разработки архитектуры защиты, интеграции технических, программных и организационных средств, а также обеспечивать эффективное функционирование и развитие комплексных систем безопасности в условиях современных информационных технологий и киберугроз.

Лабораторная работа № 1

ИССЛЕДОВАНИЕ УГРОЗ И МЕТОДОЛОГИИ ОЦЕНКИ УЯЗВИМОСТИ ИНФОРМАЦИИ

Цель и содержание: провести исследование содержания понятия угрозы информации в современных системах ее обработки

Теоретическое обоснование

1.1 Определение и содержание понятия угрозы информации в современных системах ее обработки

Под угрозой информации в автоматизированных системах обработки данных (АСОД) понимают меру возможности возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию:

нарушение (или опасность нарушения) физической целостности, логической структуры, несанкционированная модификация (или опасность такой модификации) информации, несанкционированное получение (или опасность такого получения) информации, несанкционированное размножение информации.

К настоящему времени известно большое количество разноплановых угроз

различного происхождения, таящих в себе различную опасность для информации. Системная их классификация приведена в таблице 1.1.

Ниже приводится краткий комментарий к приведенным в таблице 1.1 параметрам классификации, их значениям и содержанию.

Таблица 1.1 – Системная классификация угроз информации

Параметры классификации	Значения параметров	Содержание значения критерия
1 . Виды	1. 1. Физической целостности	Уничтожение (искажение)
	1. 2. Логической структуры	Искажение структуры
	1 .3. Содержания	Несанкционированная модификация
	1 .4. Конфиденциальности	Несанкционированное получение
	1 .5. Права собственности	Присвоение чужого права
2. Природа происхождения	2. 1 . Случайная	Отказы Сбои Ошибки Стихийные бедствия Побочные влияния
	2.2. Преднамеренная	Злоумышленные действия людей
3.Предпосылки появления	3. 1 . Объективные	Количественная недостаточность элементов системы Качественная недостаточность элементов системы
	3.2. Субъективные	Разведорганы иностранных государств Промышленный шпионаж Уголовные элементы Недобросовестные сотрудники
4.Источники угроз	4. 1 . Люди	Посторонние лица Пользователи Персонал

	4.2. Технические устройства	Регистрации Передачи Хранения Переработки Выдачи
	4.3. Модели, алгоритмы, программы	Общего назначения Прикладные Вспомогательные
	4.4. Технологические схемы обработки	Ручные Интерактивные Внутримашинные Сетевые
	4.5. Внешняя среда	Состояние атмосферы Побочные шумы Побочные сигналы

1. Виды угроз. Данный параметр является основополагающим, определяющим целевую направленность защиты информации.

2. Происхождение у гроз. В таблице 1.1 выделено два значения данного параметра: случайное и преднамеренное. При этом под *случайным* понимается такое происхождение угроз, которое обусловливается спонтанными и не зависящими от воли людей обстоятельствами, возникающими в системе обработки данных в процессе ее функционирования. Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния.

Сущность перечисленных событий определяется следующим образом:

а) *отказ* – нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций

б) *сбой* – временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

в) *ошибка* – неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

г) *побочное влияние* – негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обусловливается злоумышленными действиями людей, осуществляемыми в целях реализации одного или нескольких видов угроз.

3. Предпосылки появления угроз. В таблице 1.1 названы две разновидности предпосылок: *объективные* (количественная или качественная недостаточность элементов системы) и *субъективные*

(деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются следующим образом:

а) *количественная недостаточность* - физическая нехватка одного или несколько элементов системы обработки данных, вызывающая нарушения технологического процесса обработки или/и перегрузку имеющихся элементов;

б) *качественная недостаточность* - несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

в) *деятельность разведорганов иностранных государств* - специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами. К основным видам разведки относятся: агентурная (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых доброжелателей) и техническая, включающая радиоразведку (перехват радиосредства информации, циркулирующей в радиоканалах систем связи), радиотехническую (регистрацию спецсредствами сигналов, излучаемых техническими системами) и космическую (использование космических кораблей и искусственных спутников для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации другими доступными способами;

г) *промышленный шпионаж* - негласная деятельность организации (ее

представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или похищения, а также по созданию для себя благоприятных условий в целях получения максимальных выгод;

д) *злоумышленные действия уголовных элементов* - хищение информации или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

е) *злоумышленные действия недобросовестных сотрудников* - хищение (копирование) или уничтожение информационных массивов или/и программ по эгоистическим или корыстным мотивам.

4. Источники угроз. Под источником угроз понимается непосредственный исполнитель угрозы в плане негативного воздействия ее на ин формацию. Перечень и содержание источников приведены в таблице 1.1 и в дополнительных комментариях не нуждаются.

В соответствии с изложенным взаимодействие параметров угроз может быть представлено так, как показано на рисунке 1.

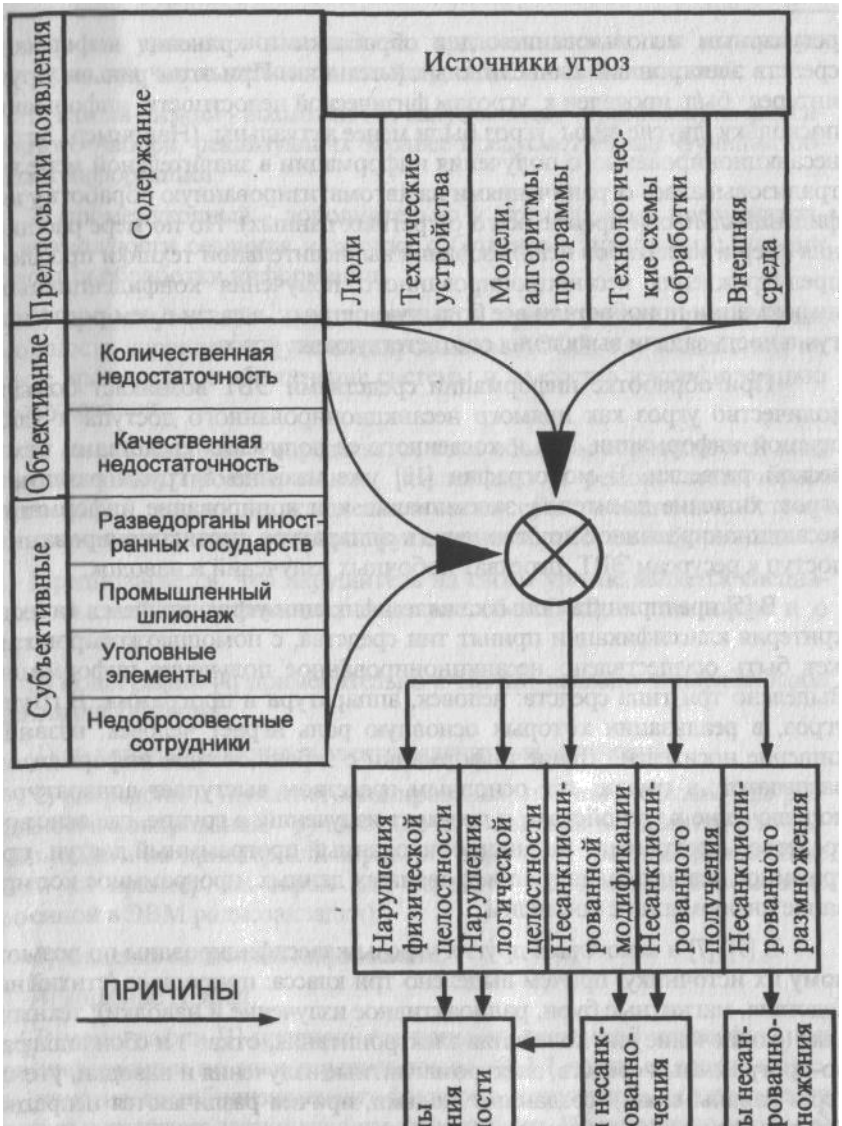


Рисунок 1.1 – Взаимодействие параметров угроз информации

Нетрудно видеть, что источники угроз и форма их проявления предопределяют возможности формирования множества причин нарушения защищенности информации по каждому из аспектов защиты. Схема такого формирования приведена на рисунке 1.1.

1.2. Ретроспективный анализ подходов к формированию множества угроз информации

Вопрос об угрозах информации возник практически одновременно с началом регулярного сбора, обработки и использования информации.

Известно, что шифрование информации в целях сохранения ее тайны применял еще древнеримский диктатор Цезарь. За многие столетия развития традиционных (бумажных) технологий выработана весьма стройная и высокоэффективная система выявления и нейтрализации угроз

Особую актуальность и новое содержание проблема формирования множества угроз приобрела в 60-е – 70-е годы нашего столетия в связи с регулярным использованием для обработки и хранения информации средств электронной вычислительной техники. При этом раньше других интерес был проявлен к угрозам физической целостности информации, поскольку другие виды угроз были менее актуальны. (Например, угроза несанкционированного получения информации в значительной мере нейтрализовывалась ограничениями на автоматизированную обработку конфиденциальных и прежде всего секретных данных). Но по мере расширения сфер и масштабов использования вычислительной техники проблемы предупреждения несанкционированного получения конфиденциальной информации приобретали все большую остроту, в связи с чем, росла и актуальность задачи выявления соответствующих угроз.

При обработке информации средствами ЭВТ возникает большое количество угроз как прямого несанкционированного доступа к защищаемой информации, так и косвенного ее получения средствами технической разведки. В современной литературе уже названо 5 групп различных угроз: хищение носителей, запоминание или копирование информации,

несанкционированное подключение к аппаратуре, несанкционированный доступ к ресурсам ЭВТ, перехват побочных излучений и наводок.

В литературных источниках предпринята попытка классификации угроз, причем в качестве критерия классификации принят тип средства, с помощью которого может быть осуществлено несанкционированное получение информации. Выделено три типа средств: человек, аппаратура и программа. В группе угроз, в реализации которых основную роль играет человек, названы: хищение носителей, чтение информации с экрана, чтение информации с распечаток; в группе, где основным средством выступает аппаратура – подключение к устройствам и перехват излучений; в группе, где основное средство – программа – несанкционированный программный доступ, программное дешифрование зашифрованных данных, программное копирование информации с носителей.

Угрозы классифицированы по возможному их источнику, причем выделено три класса: природные (стихийные бедствия, магнитные бури, радиоактивное излучение и наводки); технические (отключение или колебания электропитания, отказы и сбои аппаратно-программных средств, электромагнитные излучения и наводки, утечки через каналы связи); созданные людьми, причем различаются непреднамеренные и преднамеренные действия различных категорий лиц.

В руководящем документе Гостехкомиссии России введено понятие модели нарушителя в автоматизированной системе обработки данных, причем в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АСОД. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами, причем выделяются четыре уровня этих возможностей:

1) *самый низкий* – возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;

2) *промежуточный* – дополнительно к предыдущему предполагает возможности управления функционированием АСОД, т.е. воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее

оборудования;

3) *самый высокий* – определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АСОД, вплоть до включения в состав средств системы собственных технических средств с новыми функциями обработки информации.

Предполагается, что нарушитель на своем уровне является специалистом высшей квалификации, знает все об АСОД, в том числе и о средствах защиты.

Применительно к ПЭВМ известно четыре способа хищения информации

1) по каналам побочных электромагнитных излучений;

2) посредством негласного копирования, причем выделено две разновидности копирования: «ручное» (печать с экрана на принтер или вывод из памяти на принтер или экран) и «вирусное» (например, вывод из памяти на принтер, на экран или передача информации с помощью встроенной в ЭВМ радиозакладки);

3) хищение носителей информации;

4) хищение ПЭВМ.

Предпринята попытка системной классификации угроз информации по всем перечисленным целям ее защиты. Введены понятия дестабилизирующих факторов, источников их проявления и причин нарушения защищенности информации. Предложена методология формирования относительно полных множеств указанных причин и приведена структура этих множеств применительно к нарушению физической целостности информации и несанкционированному ее получению. Ввиду того, что предложенный подход представляется наиболее общим из всех разработанных к настоящему времени, в дальнейшем он будет рассмотрен более детально.

Своеобразный вид угроз представляют специальные программы, скрытно и преднамеренно внедряемые в различные функциональные программные системы и которые после одного или нескольких запусков разрушают хранящуюся в них информацию и/или совершают другие недозволенные действия. К настоящему времени известнонесколько

разновидностей таких программ: электронные вирусы, компьютерные черви, троянские кони.

Электронные вирусы – это такие вредоносные программы, которые не только осуществляют несанкционированные действия, но обладают способностью к саморазмножению, в силу чего представляют особую опасность для вычислительных сетей. Однако, для размножения им необходим носитель (файл, диск), что, естественно, создает для злоумышленников определенные трудности в осуществлении их несанкционированных действий.

Троянскими конями названы такие вредоносные программы, которые злоумышленно вводятся в состав программного обеспечения и в процессе обработки информации осуществляют несанкционированные процедуры, чаще всего - процедуры незаконного захвата защищаемой информации, например, записывая ее в определенные места ЗУ или выдавая злоумышленникам.

К *компьютерным червям* отнесены вредоносные программы, подобные по своему воздействию электронным вирусам, но не требующие для своего размножения специального носителя. Они обычно используют дополнительный вход в операционную систему, который создается для удобства ее отладки и который нередко забывают убрать по окончании отладки.

Раньше других появились и использовались в злоумышленных целях троянские кони, сведения о них относятся еще к семидесятым годам, причем наиболее распространенной несанкционированной процедурой было считывание информации с областей ЗУ, выделяемых законным пользователям. Первое сообщение о возможности создания электронных вирусов было сделано в 1984 г. на одной из Конференций по безопасности информации, а уже в 1985 г. была осуществлена вирусная атака на компьютерную систему подсчета голосов в конгрессе США, вследствие чего она вышла из строя. В 1987 г. зафиксированы факты появления вирусов в нашей стране. В настоящее время в мире ежегодно выявляется более тысячи вирусов.

О возможных последствиях таких угроз вирусного заражения можно судить

по следующему примеру. Адъюнкт Корнельского университета США 23-летний Роберт Моррис (кстати, сын сотрудника Агентства национальной безопасности США) 2 ноября 1988 г. произвел вирусную атаку на национальную сеть Milnet/Arpanet и международную компьютерную сеть Internet, в результате чего было выведено из строя около 6000 компьютеров. Вирус был введен в один из узлов сети, затем он разослал свои копии (длина 99 строк на языке Си) в другие узлы. В узле-получателе копия копировалась и выполнялась. В процессе выполнения с узла-источника копировалось остальное тело вируса. Общий размер вируса составил около 60 Кбайт. Хотя вирус не производил действий по разрушению или модификации информации, а способы ликвидации его были найдены уже на второй день, ущерб от его действия оценивался более чем в 150 тысяч долларов. Исследовательскому же центру НАСА в г. Маунтинн Вью (Калифорния) пришлось на два дня закрыть свою сеть для восстановления нормального обслуживания 52000 пользователей.

Уже такого беглого взгляда на вредоносные программы достаточно, чтобы убедиться в большой опасности их как угроз информации в современных средствах ЭВТ.

Нетрудно видеть, что в процессе формирования множества угроз достаточно четко проявилась тенденция перехода от эмпирических подходов к системно-концептуальным, научно обоснованным подходам

1.3. Цели и задачи оценки угроз информации

Оценка угроз, естественно, должна заключаться в определении значений тех показателей, которые необходимы для решения всех задач связанных с построением и эксплуатацией механизмов защиты информации. Тогда общую задачу оценки угроз можно представить совокупностью следующих составляющих:

1) обоснование структуры и содержания системы показателей, необходимых для исследования и практического решения всех задач, связанных с защитой информации;

2) обоснование структуры и содержания тех параметров, которые

оказывают существенное влияние на значения показателей уязвимости информации;

3) разработка комплексов моделей, отображающих функциональные зависимости показателей от параметров и позволяющих определять значения всех необходимых показателей уязвимости информации во всех представляющих интерес состояниях и условиях жизнедеятельности АСОД;

4) разработка методологии использования моделей определения значений показателей уязвимости при исследовании и практическом решении различных вопросов защиты, или иначе - разработка методологии оценки уязвимости информации.

1.4. Система показателей уязвимости информации

Для системной оценки уязвимости информации в АСОД необходимы показатели, которые отражали бы все требования к защите информации, а также структуру АСОД, технологию и условия автоматизированной обработки информации.

Уязвимость информации необходимо оценивать в процессах разработки и внедрения АСОД, функционирования АСОД на технологических участках автоматизированной обработки информации,
функционирования АСОД независимо от процессов обработки информации.

Уязвимость информации в процессе разработки и внедрения АСОД обусловливается уязвимостью создаваемых компонентов системы и баз данных. Особое значение на данной стадии имеет минимизация уязвимости программного обеспечения, поскольку от этого существенно зависит общая уязвимость информации в АСОД.

Условия автоматизированной обработки информации характеризуются, главным образом, совокупностью следующих параметров: структурой АСОД, чем определяется состав, подлежащих защите объектов и элементов; наличием и количеством дестабилизирующих факторов, потенциально возможных в структурных компонентах АСОД; количеством и категориями лиц, которые могут быть потенциальными нарушителями статуса защищаемой информации; режимами автоматизированной обработки

информации.

Уязвимость информации в процессе функционирования АСОД независимо от процесса обработки информации обусловливается тем, что современные АСОД представляют собою организационную структуру с высокой концентрацией информации, которая может быть объектом случайных или злоумышленных воздействий даже в том случае, если автоматизированная обработка ее не осуществляется.

Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры уязвимости информации наиболее целесообразно принять вероятность нарушения защищаемых характеристик ее при тех условиях сбора, обработки и

хранения, которые имеют место в АСОД, а также потенциально возможные размеры (математическое ожидание) нарушения защищенности информации. Конкретное содержание показателей уязвимости для различных видов защиты приведено в таблице 1.2.

Основными параметрами, определяющими вероятность нарушения защищенности информации, являются: количество и типы тех структурных компонентов АСОД, в которых оценивается уязвимость информации;

количество и типы случайных дестабилизирующих факторов, которые потенциально могут проявиться и оказать негативное воздействие на защищаемую информацию; количество и типы злоумышленных дестабилизирующих факторов, которые могут иметь место и оказать воздействие на информацию; число и категории лиц, которые потенциально могут быть нарушителями правил обработки защищаемой информации; виды защищаемой информации. В качестве возможных значений перечисленных параметров целесообразно принять следующие: «один одного типа» (вида, категории), «заданная совокупность» и «все всех типов» (видов, категорий).

Основанием именно для такой структуризации послужили следующие обстоятельства:

1) значение «один одного типа» необходимо для оценки уязвимости защищаемой информации в отдельном компоненте АСОД и относительно какого-то дестабилизирующего фактора в его единичном

проявлении;

2) значение «заданная совокупность» необходимо для обеспечения возможностей оценки уязвимости информации в некоторой выделенной части компонентов АСОД, представляющих самостоятельный интерес в условиях обработки информации. Типичным примером такой задачи является оценка уязвимости информации на вполне определенном технологическом маршруте автоматизированной обработки;

3) значение «все всех типов» необходимо для обобщенных, интегральных оценок уязвимости информации.

Таблица 1.2 – Содержание показателей уязвимости информации

Вид защиты информации	Вид дестабилизирующего воздействия на информацию	
	Случайный	Злоумышленный
Предупреждение уничтожения или искажения	Вероятность того, что под воздействием случайных факторов информация будет искажена или уничтожена	Вероятность того, что злоумышленнику удастся уничтожить или исказить информацию
	Математическое ожидание объема уничтоженной или искаженной информации	Математическое ожидание объема уничтоженной или искаженной информации
Предупреждение несанкциони-рованной модификации	Вероятность того, что под воздействием случайных факторов информация будет модифицирована при сохранении синтаксических характери-стик	Вероятность того, что злоумышленнику удастся модифицировать информацию при сохранении синтаксических характеристик
	Математическое ожидание объема модифицированной информации	Математическое ожидание объема модифицированной информации
Предупреждение несанкциони-рованного получения	Вероятность того, что под воздействием случайных факторов защищаемая информация будет получена лицами или процессами, не имеющими на это полномочий	Вероятность того, что злоумышленнику удастся получить (похитить) защищаемую информацию

	Математическое ожидание объема несанкциони-рованно полученной информации	Математическое ожидание объема похищаемой информации
Предупреждение несанкциони-рованного размножения (копирования)	Случайное несанкционированное размножение (копирование) информации в корыстных целях является маловероятным	Вероятность того, что злоумышленнику удастся несанкционированно снять копию с защищаемой информации без оставления следов злоумышленных действий
		Математическое ожидание объема несанкционированно скопированной информации
		Математическое ожидание числа несанкционированно снятых копий

Множество разновидностей различных показателей уязвимости определяется декартовым произведением чисел, характеризующих количество значений всех значащих параметров. Если не разделять дестабилизирующие факторы на случайные и злоумышленные (т. е. рассматривать их единым множеством) и не разделять защищаемую информацию на виды, то структура полного множества разновидностей показателей уязвимости может быть наглядно представлена так, как показано на рис. 1.2, из которого следует, что два показателя занимают особое положение, а именно: первый находится в самом начале выбранной системы координат, второй - в самом конце классификационной структуры, т.е. занимает крайнее положение справа, вверху и спереди.

Первый показатель обозначает уязвимость информации в одном структурном компоненте АСОД при однократном проявлении одною дестабилизирующего фактора и относительно одного потенциального нарушителя. Все другие показатели приведенного на рисунке множества могут быть выражены в виде некоторой функции этого показателя.

Второй выделенный выше показатель характеризует общую уязвимость, т. е. уязвимость информации в АСОД в целом по всем потенциально возможным дестабилизирующим факторам относительно всех потенциально

возможных нарушителей. Первый показатель назовем базовым, второй - общим. Тогда другие показатели приведенного на рис. 1.2 множества можно назвать *частично обобщенными.*

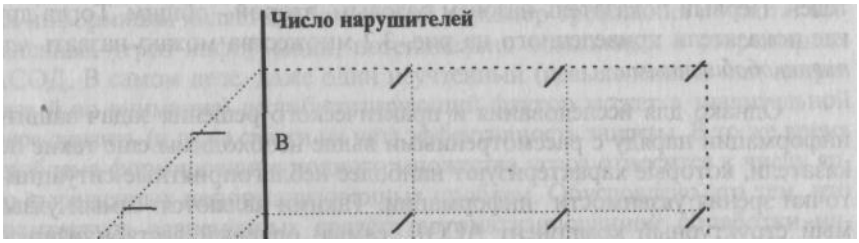


Рисунок 1.2 – Структура множества показателей уязвимости (защищенности) информации в АСОД

О - один; ЗС - заданная совокупность; В – все

Однако для исследования и практического решения задач защиты информации наряду с рассмотренными выше необходимы еще такие показатели, которые характеризуют наиболее неблагоприятные ситуации с точки зрения уязвимости информации. Такими являются: самый уязвимый структурный компонент АСОД, самый опасный дестабилизирующий фактор, самый опасный нарушитель. Эти показатели могут быть названы экстремальными.

И еще одно обстоятельство. До сих пор ничего не говорилось о том временном интервале, относительно которого оценивается уязвимость информации. А между тем совершенно очевидно, что данный параметр относится к числу существенно значимых. Вообще говоря, время является категорией сугубо непрерывной. Однако для рассматриваемых здесь целей время как параметр уязвимости информации можно структурировать, выделив такие интервалы:

1) очень малые – интервалы, которые можно считать точками;

2) малые – интервалы, которые нельзя сводить к точке, однако происходящие на них процессы можно считать однородными;

3) большие – интервалы, которые нельзя считать малыми, но на которых заранее можно определить (установить) состояние каждого структурного компонента на каждом его малом интервале;

4) очень большие – интервалы, для которых не может быть выполнено

условие больших интервалов, но на которых с достаточной точностью все же можно спрогнозировать последовательность и содержание функционирования основных компонентов АСОД;

5) бесконечные большие - интервалы, для которых не представляется возможным выполнить условие очень больших интервалов.

Например, к очень малым можно отнести интервалы времени продолжительностью до десятков минут (1-2 часа), к малым – до нескольких часов, большим – до десятков часов (нескольких суток), очень больших – до нескольких недель (месяцев), бесконечно большим - более нескольких месяцев. Заметим, однако, что размеры интервалов,вообще говоря, существенно зависят от параметров конкретных АСОД и конкретных условий их функционирования.

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Рассмотреть взаимодействие параметров угроз информации

3. Изучить систему показателей уязвимости 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. Системную классификацию угроз информации

2. Описание взаимодействия параметров угроз информации

3. Описание системы показателей уязвимости информации

4. Выводы по проделанной работе.

Вопросы для защиты работы

1. Что означает оценка угроз информации и почему она необходима.
2. Дайте определение и приведите системную классификацию угроз информации.

3. Дайте описание системы показателей уязвимости информации.

Лабораторная работа № 2

ИССЛЕДОВАНИЕ КЛАССИФИКАЦИОННОЙ СТРУКТУРЫ И СОДЕРЖАНИЯ УГРОЗ ИНФОРМАЦИИ

Цель и содержание: провести исследование классификационной структуры системы показателей уязвимости информации.

Теоретическое обоснование

Одной из наиболее принципиальных особенностей проблемы защиты информации является абсолютный характер требования полноты выявленных угроз информации, потенциально возможных в современных АСОД. В самом деле, даже один неучтенный (не выявленный или не принятый во внимание) дестабилизирующий фактор может в значительной мере снизить (и даже свести на нет) эффективность защиты. В то же время проблема формирования полного множества угроз относится к числу ярко выраженных неформализованных проблем. Обусловлено это тем, что архитектура современных средств автоматизированной обработки информации организационно-структурное и функциональное построение информационно-вычислительных систем и сетей, технология и условия автоматизированной обработки информации таковы, что накапливаемая
хранимая и обрабатываемая информация подвержена случайным влияниям чрезвычайно большого числа факторов, многие из которых должны быть

квалифицированы как дестабилизирующие.

Таким образом, возникает ситуация, когда, с одной стороны, требование необходимости решения задачи является абсолютным, а с другой регулярные методы решения этой задачи отсутствуют. Рассмотрим возможные подходы разрешения данного противоречия.

Одним из наиболее адекватных и эффективных методов формирования и особенно проверки множества потенциально возможных угроз является метод натурных экспериментов. Суть его заключается в том, что на

существующих АСОД проводятся специальные эксперименты, в процессе которых выявляются и фиксируются проявления различных дестабилизирующих факторов. При надлежащей организации экспериментов достаточной их продолжительности можно набрать статистические данные, достаточные для обоснованного решения рассматриваемой задачи. Однако постановка таких экспериментов будет чрезвычайно дорогостоящей и сопряжена с большими затратами сил и времени. Поэтому данный метод целесообразен не для первоначального формирования множества дестабилизирующихфакторов, а для его уточнения и пополнения, осуществляемого попутно с целевым функционированием АСОД

Поскольку в настоящее время отсутствуют сколько-нибудь полные и всесторонние статистические данные о дестабилизирующих факторах (задача отбора, накопления и обработки таких данных является одной из составляющих и весьма актуальных задач защиты информации, подлежащих регулярному решению), для первоначального формирования возможно более полного множества дестабилизирующих факторов наиболее целесообразно использовать экспертные оценки в различных их модификациях. Однако при этом не может быть гарантировано формирование строго полного множества дестабилизирующих факторов. Поэтому будем называть формируемое таким образом множество *относительно полным,* подчеркивая этим самым его полноту относительно возможностей экспертных методов

С учетом всего вышесказанного, структура и общее содержание алгоритма формирования относительно полного множества дестабилизирующих

факторов, влияющих на защищенность информации,

представлены на рисунке 2.1

Для доведения первоначально сформированного множества дестабилизирующих факторов до возможно большей степени полноты весьма эффективной может оказаться такая разновидность экспертных оценок, как метод психоинтеллектуальной генерации. На рисунке 2.2

приведена укрупненная схема психоэвристической программы уточнения и пополнения множества дестабилизирующих факторов по методологии психоинтеллектуальной генерации.

В соответствии с рассмотренной выше методикой сформируем относительно полное множество причин нарушения целостности информации (ПНЦИ).

Напомним, что под ПНЦИ понимаются такие дестабилизирующие факторы, следствием проявления которых может быть нарушение физической целостности информации, т.е. ее искажение или уничтожение

Классификация выявленных ПНЦИ представлена на рисунке 2.3, перечень ПНЦИ – в таблице 2.1.

Таким образом, объективно существует около 140 различных причин,

по которым может произойти нарушение целостности информации.

Однако следует иметь в виду, что многие из приведенных в таблице 2.1 ПНЦИ являются агрегированными, т. е. разделяющимися на некоторое число самостоятельных ПНЦИ. Например, ПНЦИ 1.1.1 – полный выход аппаратуры из строя - может быть разделен на выход из строя процессора, оперативного ЗУ, устройства управления ВЗУ, выход из строя печатающего устройства и т.д. Точно так же могут быть дезагрегированы многие другие ПНЦИ, поэтому общее число единичных (элементарных) ПНЦИ исчисляется несколькими сотнями.

Рассмотрим далее структуру и содержание относительно полного множества каналов несанкционированного получения информации (КНПИ).

Поскольку один из основных предметов нашего рассмотрения – защита информации от несанкционированного получения, то потенциально возможные каналы такого получения рассмотрим несколько детальней.

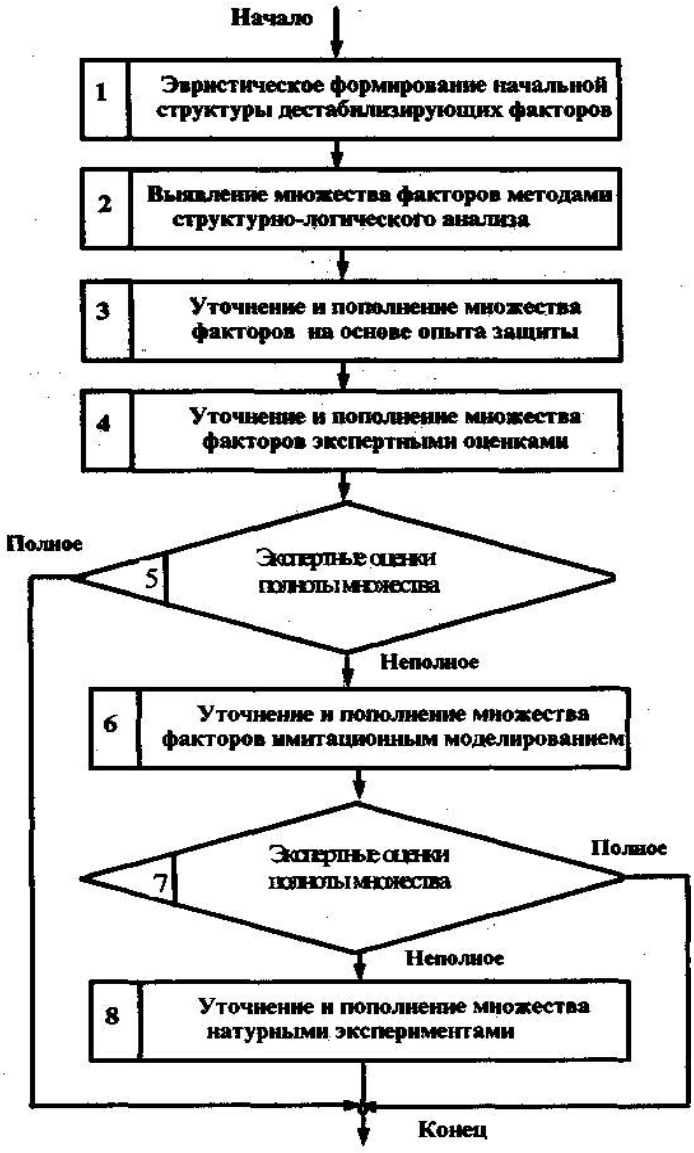


Рисунок 2.1 – Структура общего алгоритма формирования относительно полного множества дестабилизирующих факторов

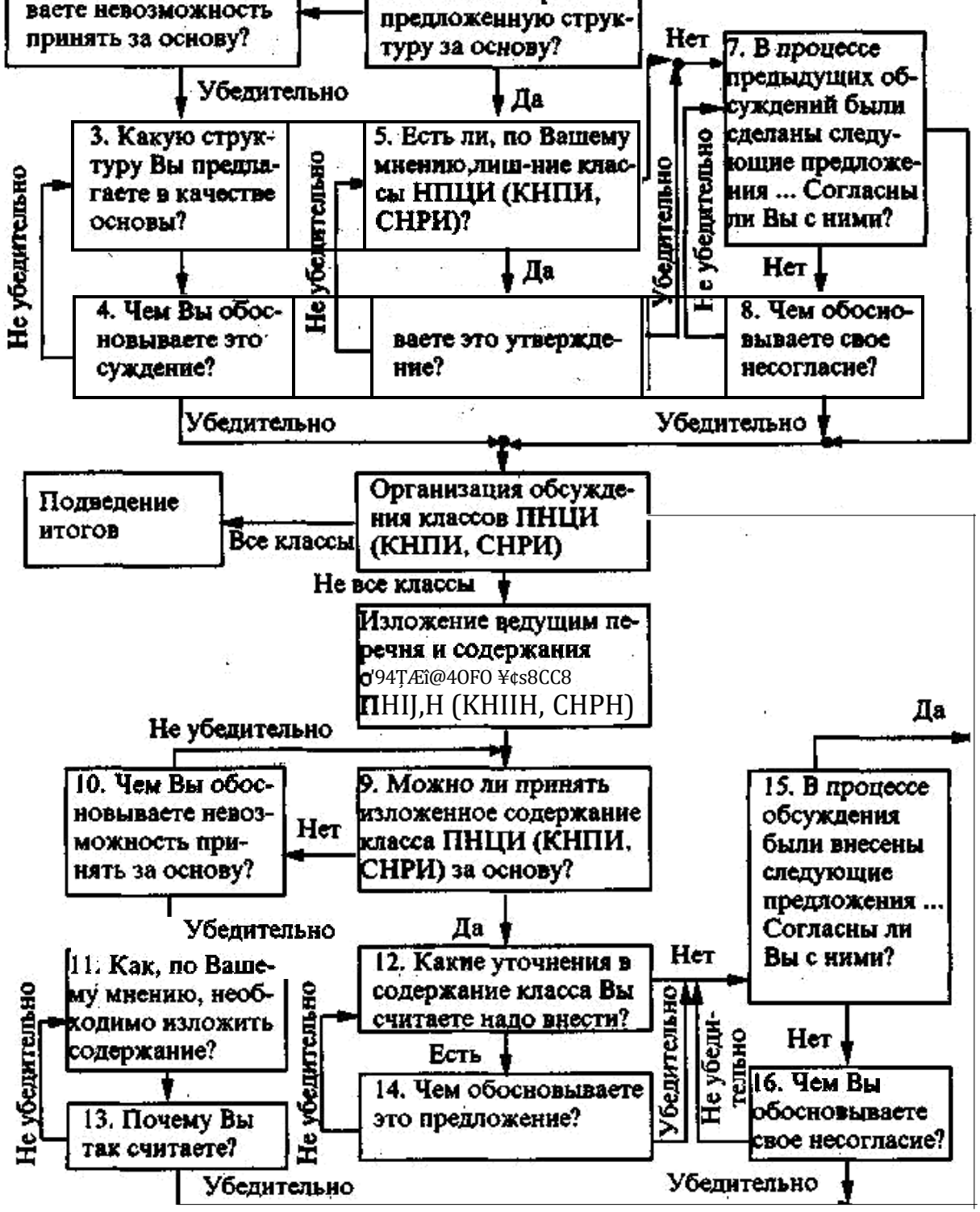

ваете невозможность принять за основу?
предложенную структуру за основу?
Нет
7. В процессе предыдущих обсуждений были сделаны следующие предложения ... Согласны ли Вы с ними?
Убедительно
Да
3. Какую структуру Вы предлагаете в качестве основы?
5. Есть ли, по Вашему мнению,лиш-ние классы НПЦИ (КНПИ, СНРИ)?
Не убедительно
Убедительно
Не убедительно
Да
Нет
4. Чем Вы обосновываете это суждение?
ваете это утверждение?
8. Чем обосновываете свое несогласие?
Убедительно
Убедительно
Подведение итогов
Все классы
Организация обсуждения классов ПНЦИ (КНПИ, СНРИ)
Не все классы
Изложение ведущим перечня и содержания
ПНIJ,Н (КНIIН, СНРН)
Не убедительно
Да
10. Чем Вы обосновываете невозможность принять за основу?
Нет
9. Можно ли принять изложенное содержание класса ПНЦИ (КНПИ, СНРИ) за основу?
15. В процессе обсуждения были внесены следующие предложения ... Согласны ли Вы с ними?
Убедительно
Да
Нет
11. Как, по Вашему мнению, необходимо изложить содержание?
12. Какие уточнения в содержание класса Вы считаете надо внести?
Нет
Не убедительно
Не убедительно
Убедительно
Не убедительно
Есть
Нет
13. Почему Вы так считаете?
14. Чем обосновываете это предложение?
16. Чем Вы обосновываете свое несогласие?
Убедительно
Убедительно

Рисунок 2.2 – Структура и содержание психоэвристической программы

уточнения множества ПНЦИ (КНПИ, СНРИ)

Рисунок 2.3 - Классификационная структура относительно полного множества ПНЦИ

Таблица 2.1 – Перечень потенциально возможных ПНЦИ

Наименование группы ПНЦИ	Наименование ПНЦИ
1.1. Отказ основной аппаратуры	1.1.1. Полный выход аппаратуры из строя 1.1.2. Неправильное выполнение функций
1.2. Отказы программ	1 .2. 1 . Искажение кода операции 1.2.2. Искажение адреса выборки 1.2.3. Искажение адреса отсылки 1.2.4. Искажение адреса передачи управления 1 .2.5. Уничтожение фрагментов программ 1 .2.6. Неправильное размещение программ в ЗУ
1 .3. Отказы людей	1.3.1. Полный выход из строя 1.3.2. Систематическое неправильное выполнение функций
1 .4. Отказы носителей ин-формации	1.4.1. Физическое разрушение носителя 1.4.2. Невосстанавливаемое ухудшение характеристик носителя
1.5. Отказы систем питания	1.5.1. Аварийное выключение питания 1.5.2. Повреждение линий электропитания 1.5.3. Невосстанавливаемое повышение напряжения 1.5.4. Невосстанавливаемое понижение напряжения 1.5.5. Невосстанавливаемое изменение частоты тока
1.6. Отказы систем обеспечения нормальных условий работы аппаратуры и персонала	1.6.1. Отключение систем кондиционирования 1.6.2. Невосстанавливаемое снижение производитель-ности систем кондиционирования 1.6.3. Необеспечение системой кондиционирования необходимой производительности 1.6.4. Отключение других систем обеспечения нор-мальных условий работы аппаратуры и персонала
1.7. Отказы систем передачи данных	1.7.1. Полный выход из строя канала связи 1.7.2. Полный выход из строя средств связи 1.7.3. Неправильное выполнение функций каналом связи 1.7.4. Неправильное выполнение функций средствами связи
1.8. Отказы вспомогательных материалов	1.8.1. Неисправимые дефекты красящей ленты 1.8.2. Неисправимые дефекты бумаги для устройства печати
2. 1. Сбои основной	2. 1 . 1 . Неправильное выполнение функций

аппаратуры	

Наименование группы ПНЦИ	Наименование ПНЦИ
2.2. Сбои программ	2.2.1. Неправильное выполнение кода операций 2.2.2. Неправильное исполнение адреса выборки 2.2.3. Неправильное исполнение адреса отсылки 2.2.4. Неправильное исполнение адреса передачи управления
2.3. Сбои людей	2.3.1. Временный выход из строя 2.3.2. Эпизодическое неправильное выполнение функций
2.4. Сбои носителей информации	2.4.1. Восстанавливаемое ухудшение характеристик носителя
2.$. Сбои систем питания	2.5. 1 . Кратковременное выключение питания 2.5.2. Кратковременное повышение напряжения 2.5.3. Кратковременное понижение напряжения 2.5.4. Кратковременное изменение частоты тока
2.6. Сбои систем обеспечения нормальных условий работы	2.6.1. Кратковременное отключение систем кондиционирования 2.6.2. Кратковременное снижение производительности систем кондиционирования 2.6.3. Кратковременное отключение других систем обеспечения нормальных условий работы аппаратуры и персонала
2.7. Сбои систем передачи данных	2.7.1 . Неправильное выполнение функций каналом связи 2.7.2. Неправильное выполнение функций средствами связи
2.8. Сбои вспомогательных материалов	2.8.1 . Исправимые дефекты красящей ленты 2.8.2. Исправимые дефекты бумаги
3. 1 . Ошибки основной аппа-ратуры	3.1.1 . Неправильный монтаж схемы процедуры 3.1.2. Неправильный монтаж схемы перехода к процедуре 3.1.3. Неправильный монтаж схемы адреса выборки 3.1.4. Неправильный монтаж схемы адреса отсылки
3.2. Ошибки программ	3.2.1. Неправильный код операции 3.2.2. Неправильный адрес выборки 3.2.3. Неправильный адрес отсылки 3.2.4. Неправильная передача управления 3.2.5. Неправильное расположение фрагментов программ
3.3. Ошибки людей	3.3. 1 . Неправильное восприятие информации 3.3.2, Неправильный набор информации 3.3.3. Неправильный выбор процедуры

	3.3.4. Случайное вмешательство в процесс
Наименование группы ПНЦИ	Наименование ПНЦИ
3.4. Ошибки систем передачи данных	3.4.1. Неправильная схема коммутации канала 3.4.2. Неправильная схема коммутации в канале 3.4.3. Неправильный монтаж схемы в устройствах связи
4.1. Пожар	4.1.1. Небольшой (локальный) 4.1.2. Средний 4.1.3. Общий (большой)
4.2. Наводнение	4.2.1. Местное (локальное) 4.2.2. Среднее (в пределах здания) 4.2.3. Общее (городское)
4.3. Землетрясение	4.3.1. Легкое 4.3.2. Среднее 4.3.3. Сильное
4.4. Ураган	4.4.1. Малый 4.4.2. Средний 4.4.3. Сильный
4.5. Взрыв	4.5.1. Легкий 4.5.2. Средний 4.5.3. Сильный
4.6. Авария	4.6.1. Небольшая 4.6.2. Средняя 4.6.3. Крупная
5.1. Хищение	5.1.1. Хищение бланков с исходными данными 5.1.2. Хищение перфокарт 5.1.3. Хищение магнитных носителей 5.1.4. Хищение выходных документов
5.2. Подмена	5.2.1. Подмена бланков 5.2.2. Подмена перфокарт 5.2.3. Подмена магнитных носителей 5.2.4. Подмена выходных документов 5.2.5. Подмена аппаратуры 5.2.6. Подмена элементов программ
5.3. Подключение	5.3.1. Подключение генераторов помех 5.3.2. Подключение регистрирующей аппаратуры
5.4. Поломка (повреждение)	5.4.1. Поломка аппаратуры 5.4.2. Повреждение программ 5.4.3. Повреждение элементов баз данных 5.4.4. Повреждение носителей 5.4.5. Повреждение документов

5.5. Диверсия	5.5.1. Создание пожара 5.5.2. Организация наводнения 5.5.3. Организация взрыва 5.5.4. Повреждение системы электропитания

Наименование группы ПНЦИ	Наименование ПНЦИ
	5.5.5. Повреждение систем обеспечения нормальных условий работы аппаратуры и персонала
6.1. Электромагнитные излучения устройств АСОД	6.1. Излучение устройств наглядного отображения 6.2. Излучение процессоров 6.3. Излучение внешних запоминающих устройств 6.4. Излучение печатающих устройств 6.5. Излучение аппаратуры связи 6.6. Излучение линий связи 6.7. Излучение вспомогательной аппаратуры
6.2. Паразитные наводки	6.2. 1 . Наводки в коммуникациях общего назначения 6.2.2. Наводки в слаботочных цепях 6.2.3. Наводки в сетях питания
6.3. Внешние электромагнитные излучения	6.3.1 . Излучения около устройств наглядного отображения 6.3.2. Излучения около внешних запоминающих устройств 6.3.3. Излучения около печатающих устройств 6.3.4. Излучения около аппаратуры связи 6.3.5. Излучения около процессоров 6.3.6. Излучения около линии связи 6.3.7. Излучения около вспомогательных устройств 6.3.8. Излучения в хранилищах носителей
6.4. Вибрация	6.4.1. Малая 6.4.2. Средняя 6.4.3. Большая
6.5. Внешние атмосферные явления	6.5.1. Изменения температуры 6.5.2. Повышение влажности воздуха 6.5.3. Повышение запыленности воздуха 6.5.4. Повышение уровня радиации 6.5.5. Заражение воздуха ядовитыми веществами 6.5.6. Бактериологическое заражение воздуха

Под *КНПИ* понимаются такие дестабилизирующие факторы, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами или процессами, не имеющими на это законных полномочий. Объективная необходимость формирования

полного множества потенциально возможных КНПИ такая же, как и для ПНЦИ, а если в АСОД обрабатывается информация повышенной секретности, то указанное требование становится практически абсолютным.

В то же время трудности формирования полного множества КНПИ значительно большие, чем при решении аналогичной задачи для ПНЦИ.

Объясняется это тем, что несанкционированное получение информации связано преимущественно с злоумышленными действиями людей, которые очень трудно поддаются структуризации. Приводимые ниже структура множества и перечень КНПИ сформированы с использованием методики,

упомянутой в начале данного параграфа.

Прежде всего, было установлено, что с целью формирования возможно более полного множества КНПИ, необходимо построить строго полную классификационную их структуру. Такая структура может быть построена,

если в качестве критериев классификации выбрать следующие два показателя: *отношение к состоянию защищаемой информации в АСОД и степень взаимодействия злоумышленника с элементами АСОД.* По первому критерию будем различать два состояния: безотносительно к обработке

(несанкционированное получение информации может иметь место даже в том случае, если она не обрабатывается, а просто хранится в АСОД) и в процессе непосредственной обработки средствами АСОД. Полная структуризация второго критерия может быть осуществлена выделением следующих его значений:

1) без доступа к элементам АСОД (т.е. косвенное получение информации);

2) с доступом к элементам АСОД, но без изменения их состояния или содержания;

3) с доступом к элементам АСОД и с изменением их содержания или состояния.

Классификационная структура КНПИ представлена на рисунке 2.4.

Таким образом, все множество потенциально возможных КНПИ может быть строго разделено на шесть классов. Полнота представленной классификационной структуры гарантируется тем, что выбранные критерии

классификации охватывают все потенциально возможные варианты взаимодействия злоумышленника с АСОД, а структуризация значений критериев осуществлялась по методу деления целого на части.

Критерии Классификации			Отношение к обработке информации	
			Проявляющиеся безотносительно к обработке	Проявляющиеся в процессе обработки
Зависимость доступа	Не требующие доступа		1-ый класс Общедоступные постоянные	2-ой класс Общедоступные функциональные
	Требующие доступа	Без изменения элементов системы	3-ий класс Узкодоступные постоянные	4-ый класс Узкодоступные , оставления следов
			5-ый класс Узкодоступные постоянные с	6-ой класс Узкодоступные оставлением следов

Рисунок 2.4 - Классификационная структура каналов несанкционированного получения информации

Следующим шагом на пути решения рассматриваемой задачи является обоснование возможно более полного перечня КНПИ в пределах каждого из шести классов. Это может быть осуществлено преимущественно эвристическими методами, в силу чего полнота полученных перечней не

гарантирована. Поэтому сформированное множество КНПИ является полным лишь относительно, т. е. лишь относительно имеющейся степени познания природы появления каналов получения информации.

Сформированные перечни выглядят следующим образом.

КНПИ 1-го класса – каналы, проявляющиеся безотносительно к обработке информации и без доступа злоумышленника к элементам ЭВТ:

1) хищение носителей информации на заводах, где производится их ремонт;

2) подслушивание разговоров лиц, имеющих отношение к АСОД;

3) провоцирование на разговоры лиц, имеющих отношение к АСОД;

4) использование злоумышленником визуальных средств;

5) использование злоумышленником оптических средств;

6) использование злоумышленником акустических средств.

КНПИ 2-го класса – каналы, проявляющиеся в процессе обработки информации без доступа злоумышленника к элементам АСОД:

1) электромагнитные излучения устройств наглядного отображения;

2) электромагнитные излучения процессоров;

3) электромагнитные излучения внешних запоминающих устройств;

4) электромагнитные излучения аппаратуры связи;

5) электромагнитные излучения линий связи;

6) электромагнитные излучения вспомогательной аппаратуры;

7) электромагнитные излучения групповых устройств ввода-вывода информации;

8) электромагнитные излучения устройств подготовки данных;

9) паразитные наводки в коммуникациях водоснабжения;

10) паразитные наводки в системах канализации;

11) паразитные наводки в сетях теплоснабжения;

12) паразитные наводки в системах вентиляции;

13) паразитные наводки в шинах заземления;

14) паразитные наводки в цепях часофикации;

15) паразитные наводки в цепях радиофикации;
16) паразитные наводки в цепях телефонизации;

17) паразитные наводки в сетях питания по цепи 50 Гц;

18) паразитные наводки в сетях питания по цепи 400 Гц;

19) подключение генераторов помех;

20) подключение регистрирующей аппаратуры;

21) осмотр отходов производства, попадающих за пределы контролируемой зоны.

КНПИ 3-го класса – каналы,, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АСОД, но без изменения последних:

1) копирование бланков с исходными данными;

2) копирование перфоносителей;

3) копирование магнитных носителей;

4) копирование с устройств отображения;

5) копирование выходных документов;

6) копирование других документов;

7) хищение производственных отходов.

КНПИ 4-го класса – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АСОД, но без

изменения последних:

1) запоминание информации на бланках с исходными данными;

2) запоминание информации *с* устройств наглядного отображения;

3) запоминание информации на выходных документах;

4) запоминание служебных данных;

5) копирование (фотографирование) информации в процессе обработки;

6) изготовление дубликатов массивов и выходных документов;

7) копирование распечатки массивов;

8) использование программных ловушек;

9) маскировка под зарегистрированного пользователя;

10) использование недостатков языков программирования;

11) использование недостатков операционных систем;

12) использование пораженности программного обеспечения вредоносными закладками.

КНПИ 5-го класса – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам ЭВТ с изменением последних:

1) подмена бланков;

2) подмена перфоносителей;

3) подмена магнитных носителей;

4) подмена выходных документов;

5) подмена аппаратуры;

6) подмена элементов программ;

7) подмена элементов баз данных;

8) хищение бланков с исходными данными;

9) хищение перфоносителей;

10) хищение магнитных носителей;

11) хищение выходных документов;

12) хищение других документов;

13) включение в программы блоков типа «троянский конь», «бомба»; 14) чтение остаточной информации в ОЗУ после выполнения санкционированных запросов.

КНПИ 6-го класса – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к объектам ЭВТ с изменением элементов ЭВТ:

1) незаконное подключение к аппаратуре;

2) незаконное подключение к линиям связи;

3) снятие информации на шинах питания устройств наглядного отображения;

4) снятие информации на шинах питания процессоров;

5) снятие информации на шинах питания аппаратуры связи;

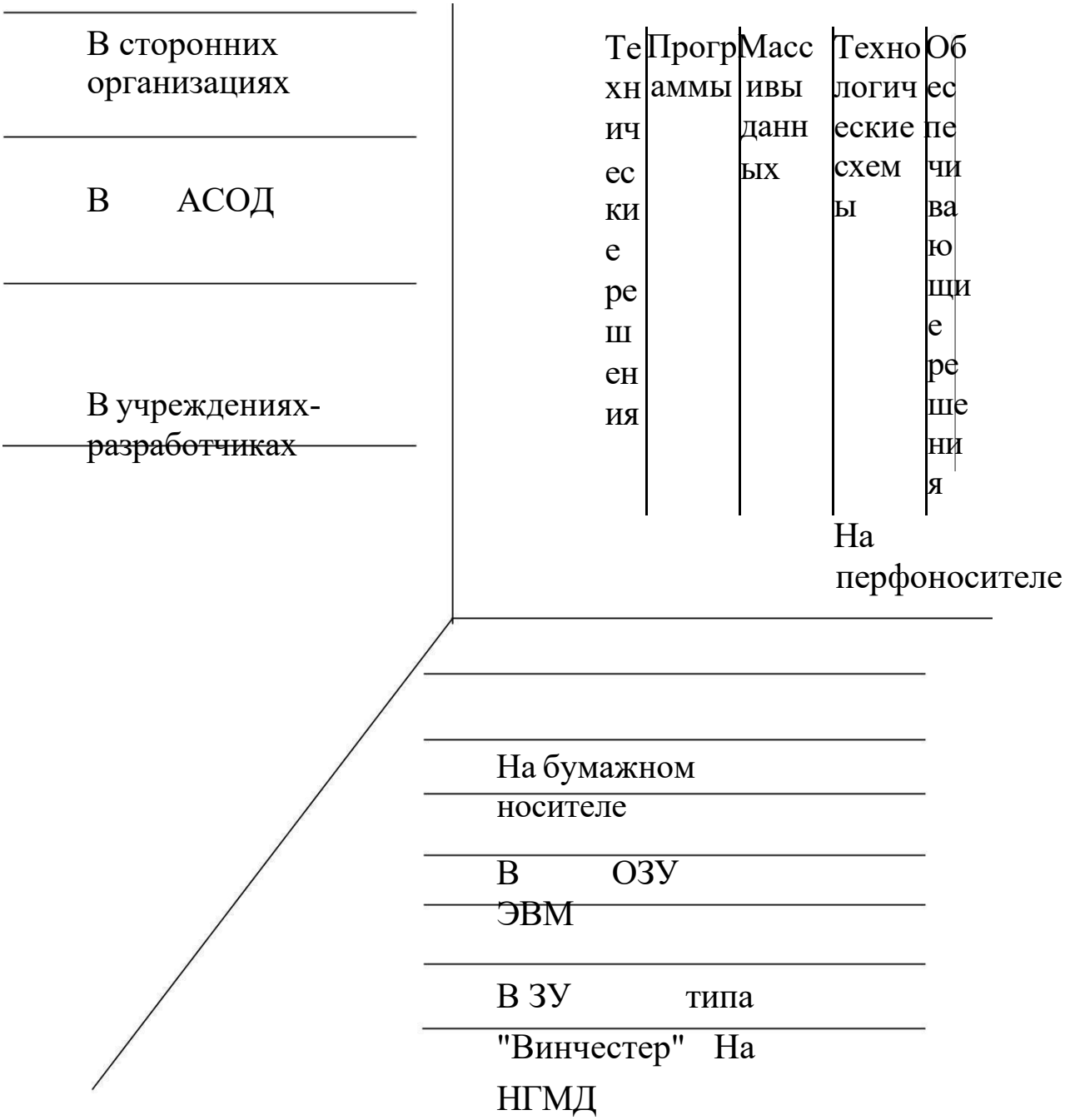
6) снятие информации на шинах питания линий связи;

7) снятие информации на шинах питания печатающих устройств;

8) снятие информации на шинах питания внешних запоминающих устройств;

9) снятие информации на шинах питания вспомогательной аппаратуры.

Местонахождение компонентов



Защищаемые компоненты

Форма представления компонентов

Рисунок 2.5 – Классификационная структура способов несанкционированного размножения информации

Классификация возможных угроз (способов) несанкционированного размножения информации приведена на рисунке 2.5

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Рассмотреть классификационную структуру каналов несанкционированного получения информации

3. Рассмотреть классификационную структуру способов несанкционированного размножения 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. Структура общего алгоритма формирования относительно полного множества дестабилизирующих факторов

2. Перечень потенциально возможных ПНЦИ

3. Описание классификационной структуры каналов несанкционированного получения информации

4. Описание классификационной структуры способов несанкционированного размножения информации

5. Выводы по проделанной работе.

Вопросы для защиты работы

1. Приведите и обоснуйте классификационную структуру каналов несанкционированного получения информации.

2. Приведите примеры конкретных каналов несанкционированного получения информации каждого класса.

Лабораторная работа № 3

ИССЛЕДОВАНИЕ МЕТОДОВ И МОДЕЛЕЙ ОЦЕНКИ УЯЗВИМОСТИ ИНФОРМАЦИИ

Цель и содержание: провести исследование методов и моделей оценки уязвимости информации

Теоретическое обоснование

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в АСОД средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в АСОД в самом общем виде представлена на рисунке 3.1. Данная модель детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размнож

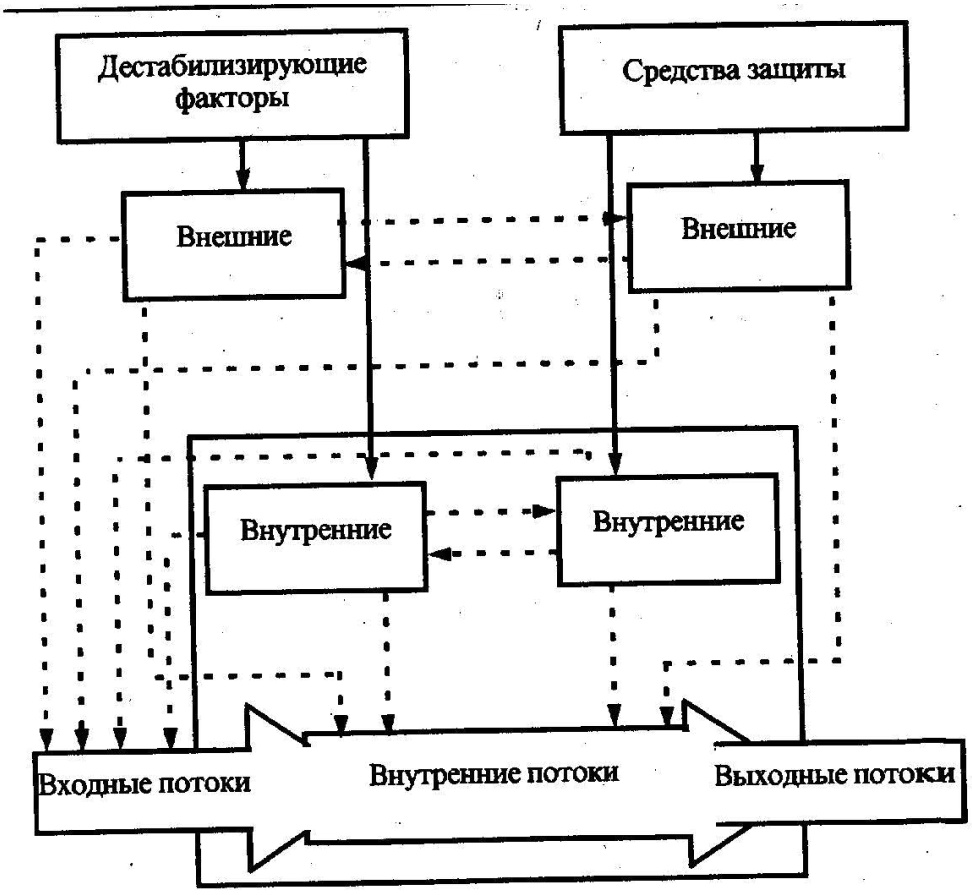


Рисунок 3.1 – Общая модель воздействия на информацию

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации в каждом объекте АСОД существенно зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход.

Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов АСОД), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений АСОД и их оборудования. Что касается злоумышленных действий, то они связаны, главным образом, с несанкционированным доступом к ресурсам АСОД. При этом наибольшую опасность представляет занесение вирусов.

В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте АСОД может быть представлена так, как показано на рисунке 3.2.

Рисунок 3.2 – Общая модель процесса нарушения
физической целостности информации

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных АСОД оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей.

Воздействие случайных факторов само по себе не ведет к несанкционированному получению информации, оно лишь способствует появлению, КНПИ, которыми может воспользоваться злоумышленник.

Структурированная схема потенциально возможных злоумышленных действий в современных АСОД для самого общего случая представлена на рисунке 3.3.

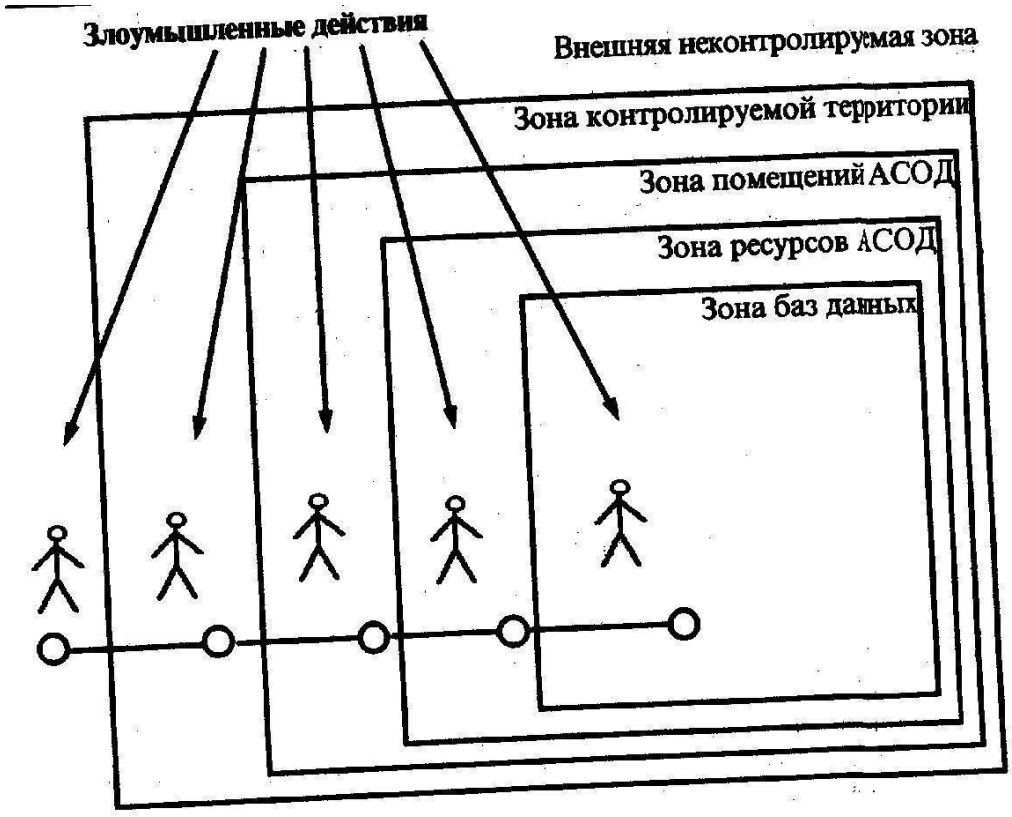


Рисунок 3.3 – Структурированная схема потенциально
возможных злоумышленных действий в АСОД

Выделенные на рисунке зоны определяются следующим образом:

1) внешняя неконтролируемая зона – территория вокруг АСОД, на которой персоналом и средствами АСОД не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;

2) зона контролируемой территории – территория вокруг помещений АСОД, которая непрерывно контролируется персоналом или средствами АСОД;

3) зона помещений АСОД – внутреннее пространство тех помещений, в которых расположены средства системы;

4) зона ресурсов АСОД – та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;

5) зона баз данных – та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий КНПИ;

соответствующий КНПИ должен быть доступен нарушителю соответствующей категории; в КНПИ в момент доступа к нему нарушителя должна находится защищенная информация.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

1) любое несанкционированное размножение есть злоумышленное действие;

2) несанкционированное размножение может осуществляться в организациях-разработчиках компонентов АСОД, непосредственно в АСОД

и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в АСОД есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной выше (см. рисунок 3.3) моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным)

попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок. Тогда модель процесса размножения в самом общем виде может быть представлена так, как показано на рисунок 3.4.

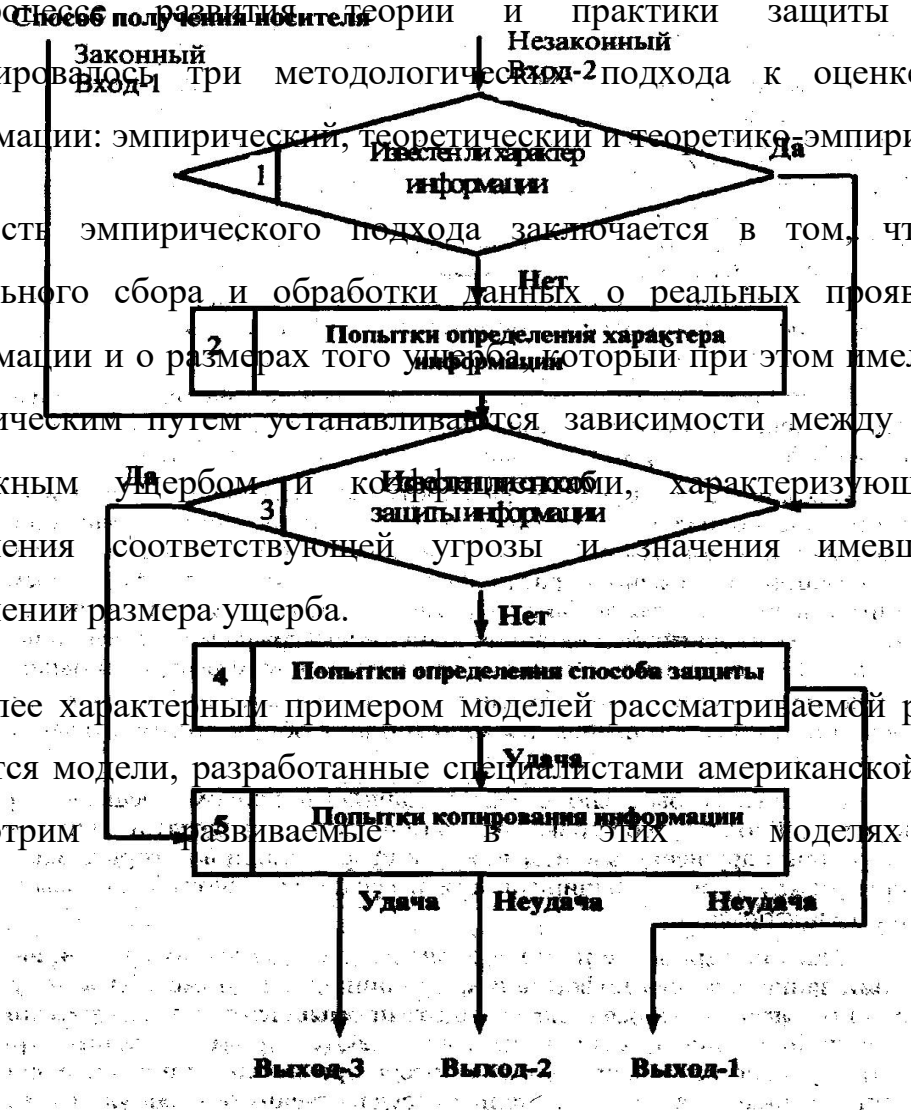
Для определения значений показателей уязвимости информации должны быть разработаны методы, соответствующие природе этих показателей и учитывающие все факторы, влияющие на их значение. На основе этих

методов должны быть разработаны модели, позволяющие рассчитывать значения любой совокупности необходимых показателей и при любых вариантах архитектурного построения АСОД, технологии и условий ее функционирования.

Ниже рассматриваются подходы к разработке названных методов и моделей.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба.



Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM. Рассмотрим развиваемые в этих моделях подходы

Рисунок 3.4 – Общая модель процесса несанкционированного копирования информации

Исходной посылкой при разработке моделей является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, с другой, обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и потерь от ее нарушения. Указанная зависимость графически представлена на рисунке 3.5. Совершенно очевидно, что оптимальным решением было бы выделение на защиту информации средств в размере C_{opt}, поскольку именно при этом обеспечивается минимизация общей стоимости защиты информации.

Для того чтобы воспользоваться данным подходом к решению проблемы, необходимо, во-первых, знать (или уметь определять) ожидаемые потери при нарушении защищенности информации, а во-вторых,

зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

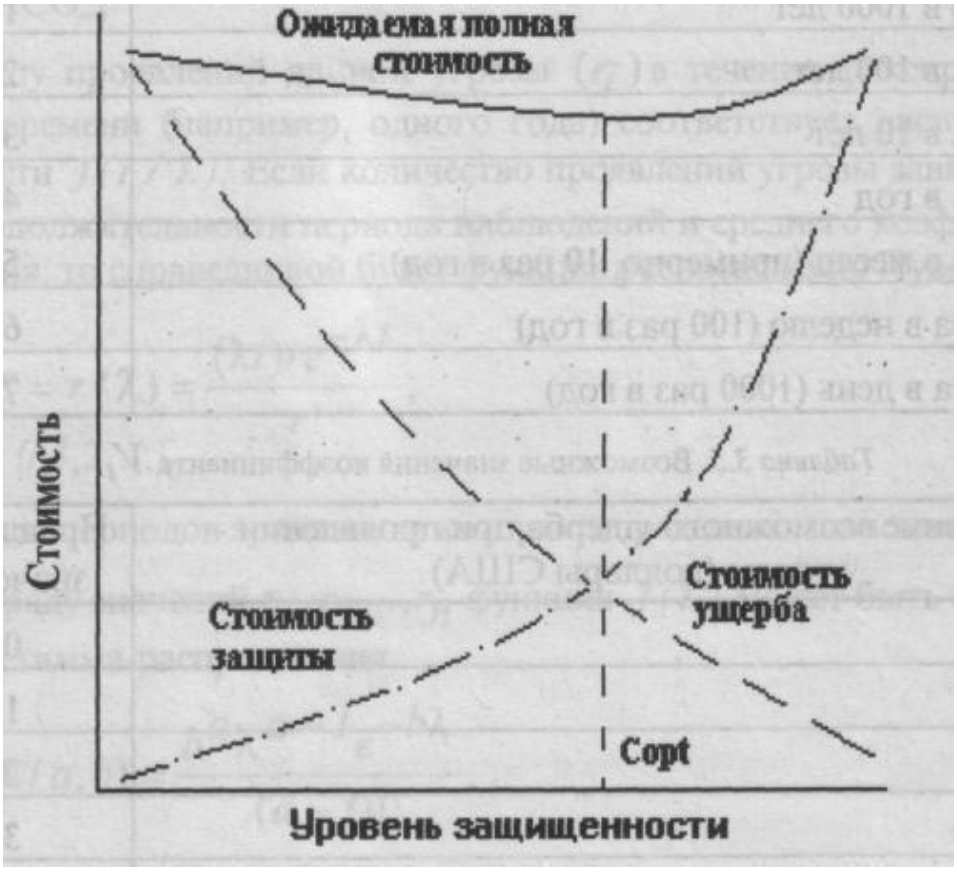


Рисунок 3.5 – Стоимостные зависимости защиты информации

Решение первого вопроса, т.е. оценки ожидаемых потерь при нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной,

коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении статуса защищенности информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования моделей, основанныхна рассматриваемых подходах.

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо по крайней мере знать, во-первых, полный перечень угроз информации, во-вторых, потенциальную опасность для информации каждой из угроз и, в-третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту (см. рисунок 3.5) состоит в том, что этот уровень должен быть равным уровню ожидаемых потерь при нарушении защищѐнности,

достаточно определить только уровень потерь. Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь от *i*-ой угрозы информации:

$$R_i = 10^{(S_i + V_i - 4)} \qquad (3.1)$$

где *Si* - коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;

V_i - коэффициент, характеризующий значение возможного ущерба при ее возникновении. Предложенные специалистами значения коэффициентов приведены в таблицах 3.1 и 3.2.

Таблица 3.1 – Значение коэффициента *Si*

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение *Si*
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
2 раза в неделю (100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 3.2 – Возможные значения коэффициента V_i

Значения возможного ущерба при проявлении угрозы (доллары США)	Предполагаемое значение V_i
1	0
10	1
100	2
1000	3
10 000	4
100 000	5
1 000 000	6
10 000 000	7

Суммарная стоимость потерь определяется формулой

$$R = \sum_{\forall i} R_i \qquad (3.2)$$

Условность и приближенность рассмотренного подхода является очевидной, и это серьезно подрывает доверие к рассматриваемой модели.

Попытки повысить адекватность модели приводят к достаточно сложным аналитическим выкладкам, основанным на методах теории вероятностей и

теории принятия решений. Для иллюстрации приведем так называемую динамическую модель оценки потенциальных угроз.

Пусть λ, есть средний коэффициент возможноѓо появления угрозы рассматриваемого типа. Для общего случая этот коэффициент рассматривается как случайная переменная λ, с распределением вероятностей $f(\lambda)$. Функция распределения должна определяться на основе обработки данных о фактах проявления угроз в процессе реального функционирования АСОД.

Числу проявлений данной угрозы (r_t) в течение фиксированного периода времени (например, одного года) соответствует распределение вероятности $f(r/\lambda)$. Если количество проявлений угрозы зависит только от продолжительности периода наблюдений и среднего коэффициента проявления, то справедливой будет функция распределения Пуассона:

$$P(r = r \mid \lambda) = \frac{(\lambda t)^r e^{-\lambda t}}{r!}; \qquad (3.3)$$

$r = 0,1,2,\ldots,$

где t - число периодов времени, за которые определены значения r.

По ряду значений $r^1, r^2, \ldots, r^n$ функция $f(\lambda)$ может быть выражена функцией гамма-распределения

$$f(\lambda \mid a, b) = \frac{b^a \lambda^{a-1} e^{-\lambda t}}{(a-1)!} \qquad (3.4)$$

где a и b - параметры распределения, определяемые по рекуррентным зависимостям:

$$a'' = a' + r^1 + r^2 + \ldots r^n$$
$$b'' = b' + t^1 + t^2 + \ldots t^n \qquad (3.5)$$

где $r^1, r^2, \ldots, r^n$ - число проявлений рассматриваемой угрозы в периоды

наблюдения $t^1, t^2, \ldots, t^n$.

Безусловное распределение вероятностей числа проявления угроз за период времени t определяется выражением

$$f(r \mid a, b, t) = \int_0^\infty f(r \mid \lambda t) f(\lambda \mid a, b) d\lambda \qquad (3.6)$$

Результирующее распределение выражается в следующем виде:

$$f_{nb}(r \mid P, a) = \frac{(r + a - 1)}{r!(a-1)} P^r (1 - P) \qquad (3.7)$$

Эффективность защиты в заданное число периодов функционирования системы характеризуется параметрами a и b. Ожидаемое количество

проявления угроз в последние t периодов характеризуется математическим ожиданием

$$E\left(r_{/b}^{-t}\right) = \underline{at} \qquad (3.8)$$

и дисперсией

$$V = (r\,t) = \begin{matrix} at \\ b(t+b) \end{matrix} \qquad (3.9)$$

Так определяются показатели возможностей проявления угроз. Подходы к оценке стоимости проявления угроз состоят в следующем. Первоначально рассматриваются средние стоимости проявления угроз, поэтому принимается нормальная функция распределения с параметрами m и V:

$$f(m, V\,m, V, n, k) = f_n(m\,m, n, V) f_g(V\,V, X) \qquad (3.10)$$

где $f^n(\cdot)$ и $f^g(\cdot)$ нормальное и гамма-распределения вероятностей; n и X - параметры гамма-распределения.

Если в последующие t периодов времени происходит r проявлений рассматриваемой угрозы, которые приводят к ущербу в размере соответственно $x^1, x^2, ..., x^r$, то параметры распределения вероятностей ожидаемых потерь корректируются следующим образом:

$$m'' = \frac{n'm' + r\bar{x}}{n''};$$

$$V'' = \frac{X'V'n'(m')^2 + (r-1)S^2 + \frac{n''(m'')^2}{r\bar{x}}}{k}; \qquad (3.11)$$

где $n'' = n' + r;\ X'' = X' + r;\ \bar{x} = \sum x_i / r;\ S^2 = \sum (x_i - \bar{x})^2 \setminus (r-1)$

Прогнозируемое распределение для ущерба от возможного проявления рассматриваемой угрозы формируется путем выделения неопределенных параметров m и V из функции распределения вероятностей для стоимости проявления угрозы данного типа. В соответствии с этим получается

$$f_s(x\,m'', V'', K'') = \int_{-\infty}^{+\infty} \int_0^{\infty} f(x\,m, V) f(m\,m'', V'', V) f_s(V\,V', X'') dm dV, \qquad (3.12)$$

$f_s(\cdot)$ - член семейства распределения Стьюдента.

Ожидаемое изменение значения $\boldsymbol{x}$ определяются параметрами:

$E(x) = m''$

$$V(x) = X'' \qquad (3.13)$$
$$K'' - 2V''$$

Поскольку возможное число проявлений *i* -ой угрозы данного типа за данный период времени является случайной переменной (r_i) и стоимость каждого проявления этой угрозы - также случайной переменной (x_{ij}), где *j=1,2,...,r,* то ожидаемая полная стоимость угроз за *t* периодов времени ($\overline{C^t}$) определяется по формуле

$$\overline{C^t} = \sum_{i=1}^{t} \sum_{j=1}^{i} x^{ij} \qquad (3.14)$$

Ожидаемая стоимость проявления угрозы одного (i-го) типа ($\overline{C^t}$) определяется по формуле

$$\overline{C^{i,t}} = \sum_{j=1}^{r} x^{ij} \qquad (3.15)$$

Поскольку стоимости проявления угроз являются случайными величинами, для полной их оценки необходимо найти функции распределения их вероятностей.

Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач зашиты информации, причем, нетрудно видеть, что модель позволяет не только находить нужные решения, но и оценивать их точность. По России такая статистика в настоящее время практически отсутствует. В США же, например, сбору и обработке указанных данных большое внимание уделяет целый ряд учреждений

(Стенфордский исследовательский институт и др.). В результате уже получены достаточно представительные данные по целому ряду угроз,

которые могут быть положены в основу ориентировочных расчетов и для других стран.

Учитывая важность данного вопроса, представляется настоятельно актуальной организация непрерывного и регулярного сбора и обработки данных о проявлениях угроз, охватывающего возможно большее число АСОД.

Рассмотренная выше модель допускает также игровую интерпретацию, т.е. может быть приведена к постановке в терминах теории игр. Предположим, что злоумышленник затрачивает *x* средств с целью преодоления механизма защиты, на создание которого израсходовано *y* средств. Естественно, ожидаемое количество информации, получаемое злоумышленником, есть некоторая функции *I(x,y).* Если далее *f(n)* – есть ценность для злоумышленника *n* единиц информации, а *g(n)* суммарные затраты на создание и сбережение этого же числа единиц информации, то чистая прибыль злоумышленника

$$V(x,y) = f[I(x,y)] - x \qquad (3.16)$$

а потери

$$u(x,y) = g[I(x,y)] + y \qquad (3.17)$$

В соответствии с известными правилами теории игр оптимальные стратегии обеих сторон могут быть определены из условий:

$$\begin{cases} f'[I(x,y)]\, dI(x,y) = 1; \\ g'[I(x,y)]\, dI(x,y) = -1 \end{cases} \qquad (3.18)$$

$$\frac{dx}{dy}$$

В теоретическом отношении эта модель является достаточно строгой, однако для практического использования необходимо определить стоимость информации, а также построить функции *I, f* и *g* для общего случая, что в настоящее время пока является нерешенной проблемой.

Естественным продолжением моделей оценки угроз АСОД являются модели нейтрализации этих угроз, т.е. модели защиты. Наиболее общей моделью защиты является модель так называемой *системы с полным перекрытием*.

При построении данной модели в качестве исходной взята естественная посылка, состоящая в том, что в механизме защиты должно содержаться, по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации. Методика формального описания такой системы заключается в следующем:

1) составляется полный перечень объектов *O* системы, подлежащих защите;

2) составляется полный перечень потенциально возможных угроз *T* информации, т.е. возможных вариантов злоумышленных действий;

3) составленные таким образом множества объединяются в двудольный граф с соблюдением условия: ребро $\langle t^i , o^j \rangle$ существует только тогда, когда угроза t_i является реальной для объекта o_j;

4) для каждого ребра в графе определяется количественная мера соответствующей угрозы для соответствующего объекта;

5) формируется множество *M* средств зашиты информации в вычислительной системе;

6) определяется количественная мера возможности противодействия каждого средства защиты каждой из угроз. Если возможность противодействия превышает уровень угрозы, то соответствующее ребро графа исключается.

Очевидно, если множество М такое, что устраняются все ребра графа, то такая система является системой с полным перекрытием.

Одной из разновидностей теоретически строгих моделей являются модели систем разграничения доступа к ресурсам АСОД.

В самом общем виде существо этих моделей может быть представлено следующим образом; АСОД является системой множественного доступа, т.е.

к одним и тем же ее ресурсам (техническим средствам, программам, массивам данных) имеет законное право обращаться некоторое число пользователей (абонентов). Если какие-либо из указанных ресурсов объявляются защищаемыми, то доступ к ним должен осуществляться лишь

при предъявлении соответствующих полномочий. Система разграничения доступа и должна стать тем механизмом, который регулирует такой доступ.

Требования к этому механизму на содержательном уровне состоят в том, чтобы, с одной стороны, не должен быть разрешен доступ пользователям (или их процессам), не имеющим на это полномочий, а с другой - не должно быть отказано в доступе пользователям (или их процессам), имеющим соответствующие полномочия.

Рассмотрим примеры моделей названных механизмов, т.е. систем разграничения доступа. Одной из первых таких моделей было формальное описание механизма системы АДЕПТ-50. Основными структурными элементами модели являются объекты следующих типов: пользователь *u*, задание *j*, терминал *t* и файл *f*. Объект каждого типа полностью описывается заданием четырех характеристик:

A – уровень компетенции, выраженный наибольшим грифом секретности данных (для данного объекта);

C – категория доступа, выраженная набором рубрик, к данным по которым разрешен доступ для объекта;

F – полномочия, выраженные списком пользователей, имеющих доступ к объекту;

M – режим, выраженный перечнем процедур, разрешенных для соответствующего объекта.

На основе такого формального описания системы можно сформулировать систему формальных правил регулирования доступа:

1) пользователь *u* получает доступ к заданию *j* тогда и только тогда, когда $u \in U$, где *U* - множество всех пользователей, зарегистрированных в системе;

2) пользователь *u* получает доступ к терминалу *t* тогда и только тогда, когда $u \in F(t)$;

3) пользователь *u* получает доступ к файлу f тогда и только тогда, когда: $u \in F(f)$; $A(u) \geq A(f)$; $C(u) \geq C(f)$; $M(u) \geq M(f)$;

4) с терминала *t* может быть осуществлен доступ к файлу f тогда и только тогда, когда: $f(t) \geq F(f)$; $A(t) \geq A(f)$; $C(t) \geq C(f)$; $M(t) \geq M(f)$.

Нетрудно видеть, что набор подобных правил может и расширяться, и модифицироваться. На основе же совокупности правил легко построить алгоритм управления доступом к данным.

К подобному типу относится разработанная несколько позже так называемая *пятимерная модель безопасности.* Для формального описания процесса доступа к данным в условиях защиты введено пять следующих множеств: *U* - список зарегистрированных пользователей; *R* - набор имеющихся в системе ресурсов; *S* - множество возможных состояний ресурсов; *E*- набор операций над ресурсами; *A* - перечень возможных полномочий пользователей.

Вводится понятие *области безопасности* как декартового произведения перечисленных множеств.

D = UARSE.

В области безопасности могут быть выделены подобласти, соответствующие отдельным пользователям, группам пользователей, отдельным ресурсам и т.п.

Любой запрос на доступ может быть описан четырехмерным кортежем

$g = (u, r, s, e), u \in U$, где
$; r \in R; s \in S; e \in E$

Запрос получает право на доступ только в том случае, если он попадает в соответствующую подобласть области безопасности.

Описанная структуризация позволяет построить алгоритмическую процедуру управления доступом. Обобщением моделей рассмотренного выше типа является модель, в которой сформулирована и строго решена задача разграничения доступа.

Постановка задачи сформулирована следующим образец. Дана система *(A, B, g)*, в которой:

$A = (A_1, A_2, ..., A_u)$ - конечный набор субъектов (активных элементов) системы;

$B = (B^1, B^2, ..., B^v)$ - конечный набор объектов (пассивных элементов) системы; a_i - код доступа субъекта *i*;

b_j - код доступа объекта *j* (*i*, *j* - некоторые двоичные *n*-разрядные числа);

$g = g(a^i, b^i)$- механизм доступа, причем

если $g(a^i, b^j) = 1$, то субъекту i разрешается доступ к объекту У;

если $g(a^i, b^j) = 0$, то указанный доступ не разрешается.

Задача заключается в том, чтобы при заданных наборах субъектов и объектов с их ограничениями в иерархических структурах и заданном механизме доступа выбрать такое значение разрядности кода доступа *n* и определить такое распределение значений кодов доступа субъектов и объектов, чтобы обеспечивались все разрешенные доступы и минимизировалось число неразрешенных доступов.

Механизмом доступа может быть любая функция из семейства булевых функций

$$g_{b_j}(a_i,) = \sum_{k=1}^{n} f(a_{ik}, b_{ik}), \quad (3.19)$$

удовлетворяющая условию:

$$g(a^i, b^j) \begin{cases} 0, \text{ в противном случае} \\ 1, \text{ если } \sum_{k=1}^{n} f(a_{ik}, b_{ik}) \end{cases} \quad (3.20)$$

Здесь: $f(a^{ik}, b^{jk})$произвольная булева функция двух бит; a^{ik}- значение *k*-*го* бита в коде доступа *j*-*го* субъекта; bj_k - значение *k*-*го* бита в коде доступа *j*-

го объекта; *m* - порог доступа, причем *0 < m < n.*

С целью получения выражений для количественных оценок введены следующие определения:

1) пусть X и Y есть такие булевы переменные, что $X_{ij} = 1$ ($Y_{ij} = 1$) означает, что A_i, имеет разрешенный (неразрешенный) доступ к B_j иначе $x^{ij} = 0$($y^{ij} = 0$). При этом x^{ij} & $y^{ij} = 0$ для всех i $(1 \le i \le |A|)$ и всех j $(1 \le j \le |B^j|)$, где /Z / означает кардинальное число множества Z;

2) пусть X_j будет числом субъектов $A_i \in A$ имеющих разрешенный доступ к B_j, y_j - число субъектов, не имеющих такого доступа, причем:

$$x_i = \sum x^{ij} \; {}_{A_i \in A}$$

$$y_i \sum_{A_i \in A}^{y} {}^{ij} \qquad (3.21)$$

3) пусть *x(y)* есть среднее (по *B)* число субъектов, имеющих разрешенный (неразрешенный) доступ к любому $B^j \in B$, т.е.

$$x_j = \frac{\sum_{B_j \in B} x^j}{|B|}; \; y_j = \frac{\sum_{B_j \in B} y^i}{|B|} \qquad (3.22)$$

4) пусть *x(y)* будет минимальным (по *B)* числом субъектов, имеющих разрешенный (неразрешенный) доступ к любому $B^j \in B$, т.е.

$$x = \min_{B_j \in B} (x_j);$$

$$y = \min_{B_j \in B} (y_i) \qquad (3.23)$$

5) пусть *X (y)* будет максимальным (по *B)* числом субъектов, имеющих разрешенный (неразрешенный) доступ к любому $B_j \in B$, т.е.

$$x \quad \max_{B_j \in B} (x_j);$$

$$y \quad \max_{B_j \in B} (v_j) \qquad (3.24)$$

Тогда качество распределения кодов доступа может быть оценено следующими показателями:

1) абсолютной степенью защиты

$$\delta_{абс} = (1+y)^{-1} \qquad (3.25)$$

При этом $\delta_{абс}=1$ будет только тогда, когда найдено такое распределение, при котором неразрешенных доступов нет вообще; в противном случае $\delta_{абс}<1$. Абсолютность данного показателя интерпретируется в том смысле, что его значение не зависит от количества субъектов и объектов, а меняется только в зависимости от среднего числа неразрешенных доступов; 2) относительной степенью защиты

$$\delta_{отн} = \frac{|A| - \bar{x} - \bar{y}}{|A| - |\bar{x}|} \qquad (3.26)$$

$0 \le \delta_{отн} \le 1$, причем $\delta_{отн}=1$, если система не допускает неразрешенных доступов, а $\delta_{отн}=0$, если система позволяет максимально возможное число неразрешенных доступов; 3) минимальной степенью защиты

$$\delta = (1+y)^{-1} \qquad (3.27)$$

4) максимальной степенью защиты

$$\delta = (1+y)^{-1} \qquad (3.28)$$

Доказано, что оптимальное распределение кода будет при минимальном числе наборов, разрешающих доступ. Это достигается при равномерном распределении субъектов по всем классам доступа.

Ниже приводятся результаты применения модели к иерархическим системам, причем под иерархическими понимаются такие системы, в которых данный субъект имеет разрешенный доступ ко всем объектам, доступ к которым имеют субъекты, стоящие в иерархии ниже данного.

Рассмотрены три вида иерархии:

1) кольцевая структура, в которой субъекты представлены совокупностью концентрических колец, причем субъект, относящийся к внутреннему кольцу, имеет разрешенный доступ ко всем объектам, к

которым имеют разрешенный доступ все субъекты, относящиеся к внешним (относительно данного) кольцам, а доступ в обратном направлении не должен разрешаться;

2) двоичная симметричная структура типа дерева, в которой каждый субъект представлен только одним узлом дерева, причем каждый субъект должен иметь разрешенный доступ ко всем объектам, к которым имеют разрешенный доступ все субъекты, расположенные ниже данного в иерархической структуре, но не имеют доступа к объектам, к которым имеют доступ субъекты более высоких уровней иерархии;

3) произвольные структуры с частичным упорядочением.

Для названных видов иерархии получены следующие результаты:

1) в системах с кольцевой структурой, в которых выполняется условие */B/=/A/=U,* с монотонным механизмом доступа при $S^{mn}(f) \le U$ присвоение кода, удовлетворяющего сформулированным выше условиям кольцевой структуры, максимизирует абсолютную и относительную степень защиты при выполнении следующих условий: в приложении используется $R_m^{n}(f)$ минимальных кодов объектов, где $R_m^{n}(f)$ - так называемый уровень линейной иерархии (для различных механизмов доступа вычисляется по различным зависимостям и составляет 1 - 6); присвоение кодов осуществляется шаг за шагом, начиная с внутреннего кольца, добавляя каждый раз 1 бит, для чего разработана специальная алгоритмическая процедура; субъекты по кодам доступа распределяются с максимально возможной равномерностью;

2) в системах с двоичной симметричной структурой типа дерева оптимальное (т. е. удовлетворяющее условиям доступа в иерархии и максимизирующее абсолютную и относительную степени защиты)

присвоение кодов доступа достигается итерационной процедурой, на каждом шаге которой объекты дерева делятся на два класса так, чтобы выделенные поддеревья находились в различных классах;

3) для произвольных иерархических структур с частичным упорядочением доказано, что нижней оценкой числа неразрешенных доступов

Является $n/2\,([n/d]^{цел}-1)$, где n - число узлов в иерархической структуре,

а d- число возможных кодов доступа.

Рассмотрим далее теоретико-эмпирический подход к оценке уязвимости информации.

Ранее было показано, что все необходимые показатели уязвимости могут быть вычислены на основе так называемых базовых показателей.

По определению, базовым является показатель уязвимости информации в одном структурном компоненте АСОД относительно одного дестабилизирующего фактора и относительно одного нарушителя одной категории (для факторов, связанных со злоумышленными действиями людей).

Для определения базовых показателей уязвимости различных видов применяются так называемые аналитические модели, которые позволяют определять искомые величины (в данном случае - показатели уязвимости информации) путем проведения вычислений по заранее установленным

(выведенным) зависимостям.

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Рассмотреть общую модель воздействия на информацию

3. Рассмотреть общую модель процесса нарушения физической целостности информации

4. Рассмотреть структурированную схему потенциально возможных злоумышленных действий в АСОД

5. Ознакомиться с общей моделью процесса несанкционированного копирования информации

6. Оформить отчет

Содержание отчета и его форма

Отчет должен иметь форму согласно оформлению простого реферата.

Титульный лист должен включать название дисциплины, название практическйо работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической работы должна содержать:

1. Определение уязвимости информации
2. Описание общей модели воздействия на информацию
3. Описание модели процесса нарушения физической целостности информации
4. Описание структурированной схемы потенциально возможных злоумышленных действий в АСОД
5. Описание модели процесса несанкционированного копирования информации
6. Характеристика стоимостных зависимостей защиты информации
7. Выводы по проделанной работе.

Вопросы для защиты работы

1. В чем особенности эмпирического подхода к оценке угроз.
2. Приведите общую модель несанкционированных действий злоумышленника

3. ц
4. P^{ijk}
5.
6. ц
7. P^{ijk}
8. i в х
9. P
10.
11. ц

Лабораторная работа № 4

ИССЛЕДОВАНИЕ АНАЛИТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОПРЕДЕЛЕНИЯ БАЗОВЫХ ПОКАЗАТЕЛЕЙ УЯЗВИМОСТИ ИНФОРМАЦИИ

Цель и содержание: провести исследование аналитических моделей для определения базовых показателей уязвимости информации

Теоретическое обоснование

Для определения базовых показателей уязвимости различных видов применяются так называемые аналитические модели, которые позволяют определять искомые величины (в данном случае - показатели уязвимости информации) путем проведения вычислений по заранее установленным

(выведенным) зависимостям.

Ниже приводятся некоторые такие аналитические модели:

а) ***Нарушение физической целостности информации.*** В соответствии с приведенной на рисунке 4.1 общей моделью процесса нарушения физической целостности информации введем следующие

изменяет поступает информация нарушений целостности

вероятность того, что целостность информации, находящейся (обрабатываемой, хранимой, передаваемой) в *i*-м структурном компоненте, будет нарушена под воздействием *j*-го дестабилизирующего фактора и (в случае злоумышленных действий людей) относительно одного нарушителя *k*-

й категории. Для тех дестабилизирующих факторов, которые не связаны со злоумышленными действиями людей, индекс «*k*» игнорируется, т.е. значения для всех *k* одинаковы и зависят только от *i* и *j*; $P^{ц}_{ijk\ вых}$ - вероятность того, что целостность выходящей из *i*-го компонента информации нарушена под воздействием *j*-го дестабилизирующего фактора и (в случае злоумышленных действий людей) относительно одного нарушителя *k*-й категории (относительно индекса «*k*» справедливо высказанное выше замечание).

Рисунок 4.1 – Общая модель процесса нарушения физической целостности информации

Нас, естественно, интересует наличие нарушения целостности выходной информации, т.е. величина $P^{ц}_{вых}$. В соответствии с теоремой умножения вероятностей случайных событий эта величина может быть

$P^{ц}_{вых} = 1 - [1 - P^{ц}_{ijk}] \cdot [1 - \cdot]$

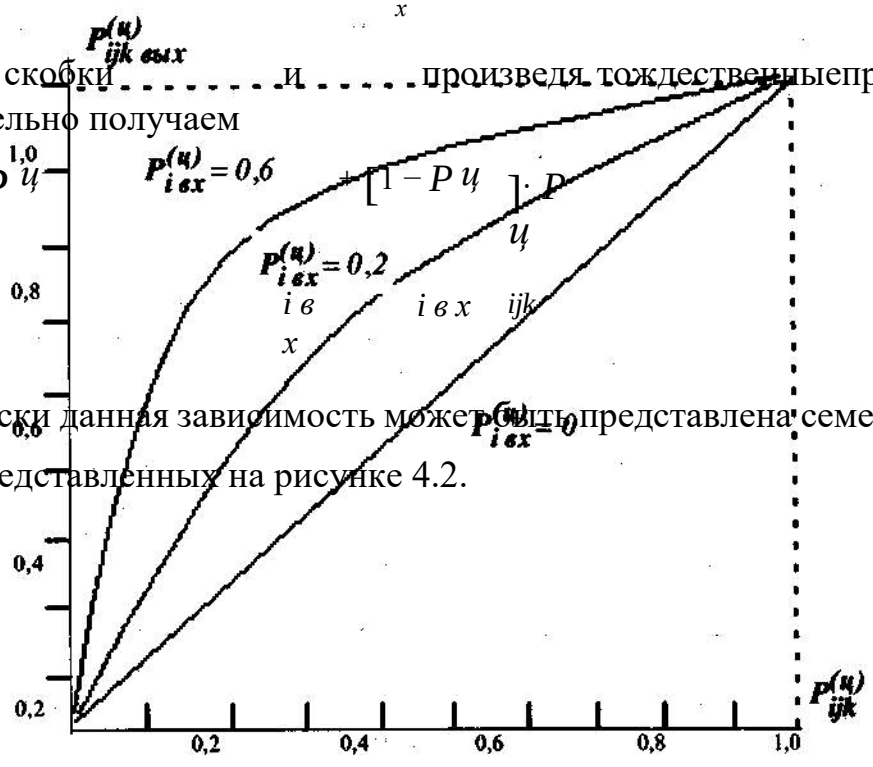
выражена следующей зависимостью:

$$P^{ijk} \qquad P^{i\ в} \qquad P^{ijk} \tag{4.1}$$

$$x$$

Раскрыв скобки и произведя тождественныепреобразования, окончательно получаем

$$P_{ijk}^{(u)} = P_{i\,вх}^{(u)} + \left[1 - P_{i\,вх}^{(u)}\right] \cdot P_{i\,вх\,ijk}^{(u)} \tag{4.2}$$



Графически данная зависимость может быть представлена семейством квых, представленных на рисунке 4.2.

ц

P^{ijk}

Рисунок 4.2 – График значений базовой вероятности нарушения физической целостности информации

Нетрудно видеть, что здесь молчаливо предполагается:

1)различные дестабилизирующие факторы воздействуют на информацию независимо один от другого;

2) процесс нарушения целостности в компоненте АСОД не зависит от того, нарушена ли целостность информации, поступающей на его вход.

Правомерность и допустимые рамки таких предположений должны быть обоснованы.

События - являются сложными в том смысле, что для их осуществления необходимо одновременное проявление соответствующего дестабилизирующего фактора и собственно нарушение целостности информации при проявлении этого фактора. Если вероятность первого события обозначить через $P^{ц,п}_{ijk}$ второго – через $P^{ijk}_{ц,н}$, то

$$P^{ijk}_{ц} = P^{ijk}_{ц,п} \cdot P^{ijk}_{ц,н} \quad (4.3)$$

Подставляя это выражение в (4.2), получаем

$$P^{ijk}_{вых} = P^{i}_{вх} + \left[1 - P^{i}_{вх}\right] \cdot P_{ijk} \qquad (4.4)$$

Значение $P^{ijk}_{вых}$ и есть базовый показатель уязвимости с точки зрения нарушений целостности выходной информации. Однако для его использования необходимы значения для всех компонентов АСОД и всех дестабилизирующих факторов. Значений этих величин в настоящее время пока нет и формирование всего их множества сопряжено с большими трудностями.

б) ***Несанкционированное получение информации.*** С точки зрения несанкционированного получения информации главную опасность представляют злоумышленные действия людей. Общая модель таких действий приведена на рис. 4.3. В соответствии с этой моделью введем следующие обозначения: P^{ikl} - вероятность доступа нарушителя *k*-й категории в *l*-ю зону *i*-го компонента АСОД; $P^{n,к}_{ijl}$ - вероятность наличия (проявления) *j*-го КНПИ в *l*-и зоне *i*-го компонента АСОД; $P^{n,н}_{ijkl}$ - вероятность доступа нарушителя *k*-й категории к *j*-му КНПИ в *l*-й зоне *i*-го компонента при условии доступа нарушителя в зону; $P^{n,и}_{ijl}$ - вероятность наличия защищаемой информации в *j*-м КНПИ в *l*-й зоне *i*-го компонента в момент доступа туда нарушителя.

Тогда в соответствии с теоремой умножения вероятностей, вероятность несанкционированного получения информации нарушителем *k*-й категории по *j*-му КНПИ в *l*-й зоне *i*-го структурного компонента АСОД определится следующей зависимостью:

$$P^{ijkl} = P^{ikl} \cdot P^{ijl} \cdot P^{(n,l)} \cdot P^{(n,д)} \cdot P^{(n,к)} \cdot P^{(n,н)}_{ij} \cdot P^{(n,и)} \quad (4.5)$$

Но поскольку под базовым показателем уязвимости информации (с точки зрения несанкционированного получения) мы условились понимать вероятность несанкционированного получения информации в одном

компоненте АСОД одним злоумышленником одной категории по одному КНПИ, то выражение для базового показателя запишется так:

$$P^{ijk} = 1 - \prod_{l=1}^{5}\left[1 - P^{(n,б)}\right] \cdot P^{ijkl} = 1 - \prod_{l=1}^{5}\left[1 - P^{(n,б)}\right] \cdot P^{(n,д)} \cdot P^{ikl} \cdot P^{(n,к)} \cdot P^{ijl} \cdot P^{(n,н)} \cdot P^{ijkl} \cdot P^{(n,и)} \cdot P^{ijl} \quad (4.6)$$

Рассмотрим далее статистические модели определения значений базовых показателей уязвимости. В силу целого ряда объективных причин далеко не всегда можно рассчитывать на наличие надежных исходных данных, необходимых для определения рассмотренных показателей уязвимости. В качестве выхода из положения в таких ситуациях предлагается использовать статистические модели, причем для этих целей разработана унифицированная статистическая модель, рассмотренная в лекционном материале.

Рассмотрим пути и способы использования унифицированной модели для определения значений базовых показателей уязвимости информации.

Центральным блоком обобщенной схемы унифицированной модели является (см. рис. 4.4) блок 5, основное содержание которого составляет собственно имитация моделируемой системы или моделируемого процесса.

Применительно к модели определения показателей уязвимости информации структура и содержание этого блока в виде вероятностно-автоматной модели ТСК показаны на рисунке 4.5. Последовательность реализации приведенной модели представлена на рисунке 4.6.

Bxon-1

1 | **Блок подготовки модели к функционированию**

Bxon-2

Выход

2 **Блок управления проц**€COOM
ROECK8QBA0R A

3 **Блок модификации модели**

Ą ÎÎSOy OĄ¥BBB38ŁgŒ l€îŁO$Œ¢OMAfŒtBttOÎł
DpO£Ł î•Ł nOHŒf8

5 | **Блок генерирования допустимых**

6 **Блок обработки результатов моделирования**

Рисунок 4.4 – Обобщенная структура имитационной модели В свою очередь центральным блоком рассмотренной здесь модели

является блок 5.4. На вход этого блока поступают потоки заявок на автоматизированную обработку информации, потоки дестабилизирующих

факторов, под воздействием которых может быть нарушен установленный статус защищенности обрабатываемой информации, а также потоки воздействий на процесс обработки информации и дестабилизирующие факторы используемых средств защиты.

В зависимости от сочетания значений параметров перечисленных потоков изменяется внутреннее состояние моделируемого объекта или процесса и формируются данные о наличии или отсутствии и масштабах нарушения защищенности информации.

Схемы процессов, подобные приведенной, удобно представлять в виде вероятностно-автоматных моделей. Применительно к реализации блока 5.4

вероятностно-автоматная модель может быть построена следующим образом.

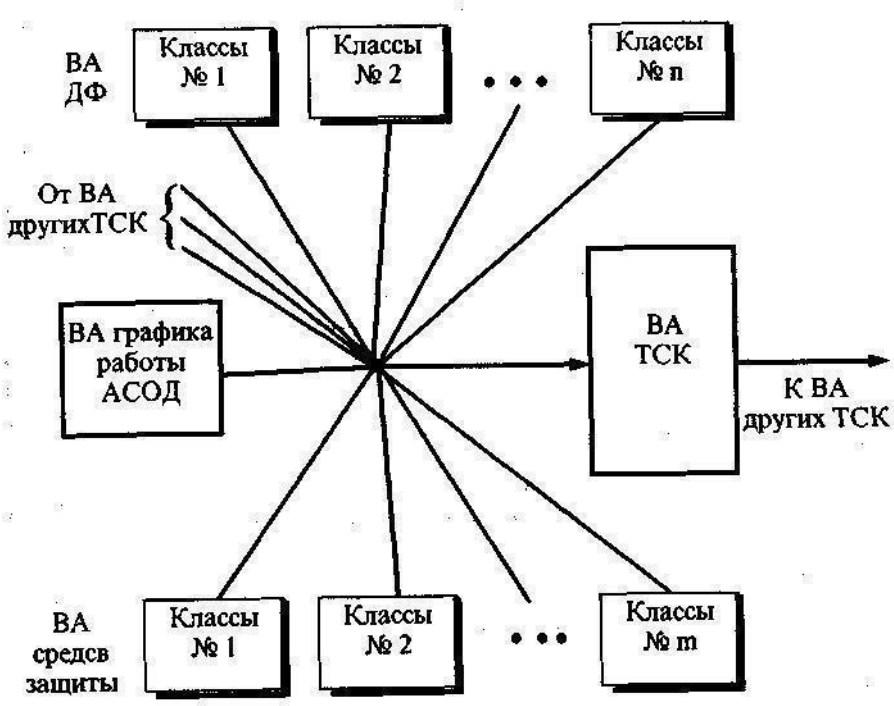


Рисунок 4.5 – Вероятностно-автоматная модель ТСК АСОД

(ВА - вероятностный автомат; ДФ - дестабилизирующий фактор)

Модель будет представлять собою совокупность взаимосвязанных вероятностных автоматов (см. рисунок 4.5), каждый из которых имитирует процесс функционирования соответствующего элемента АСОД. Поскольку

все потенциально возможные структурные элементы АСОД разделены на

типовые структурные компоненты (ТСК), структуру модели в общем случае можно представить множеством $A = \{a^i\}$, где a^i – вероятностный автомат, имитирующий работу i-го ТСК АСОД, и матрицей $/r_{i,i`}/$, где

$r_{i,i`}$ = 1, если выходные символы $i$-го автомата подаются на вход автомата $i`$

0, в противном случае

$i,i` = 1,2,\ldots,n$ (n – число ТСК в моделируемой АСОД, $i \neq i`$)

Рисунок 4.6 – Укрупненная схема модели определения показателей уязвимости информации (блок 5 обобщенной модели)

Заметим, что все однотипные ТСК могут имитироваться одним и тем же автоматом.

Далее выделяется некоторое подмножество автоматов $A^* = \{a_{i^*}\}$ $(A^* \in A)$, называемых входными, куда относятся автоматы, которые соответствуют тем ТСК, на входы которых поступают входные сигналы (терминалы, с которых вводятся запросы и/или исходные данные; каналы или аппаратура связи, участвующие в приеме запросов и/или исходных данных; терминалы администрации, с которых вводятся управляющие команды; ВЗУ, с которых считываются данные для обработки и т.п.). Выделяется также некоторое подмножество автоматов $A^{**} = \{a^{i^{**}}\}$ $(A^{**} \in A)$, называемых выходными, т.е. автоматов, соответствующих тем ТСК, выходные сигналы или внутренние состояния которых представляют интерес как результаты моделирования. При этом один и тот же автомат в общем случае может входить в оба выделенных выше подмножества. Тогда структуру вероятностно-автоматной модели АСОД в самом общем случае можно представить так, как показано на рисунке 4.7. Структура модели отдельно взятого ТСК в вероятностно-автоматном представлении приведена выше на рисунке 4.5.

Нетрудно видеть, что на базе методов вероятностно-автоматного моделирования можно построить унифицированную модель, позволяющую для АСОД любой архитектуры определять значение любого показателя уязвимости или любой их совокупности.

Базовые показатели уязвимости информации, которые могут быть определены с помощью рассмотренных выше моделей, сами по себе имеют

ограниченное практическое значение. При изучении, разработке и эксплуатации систем защиты информации необходимы значения показателей уязвимости, обобщенных по какому-либо одному индексу (*i,j* или *k)* или по их комбинации, или же характеризующих какое-либо экстремальное состояние защищенности. Полный перечень и содержание обобщенных показателей изучены ранее. Нетрудно при этом видеть, что обобщенные модели могут быть унифицированными для всех рассматриваемых здесь видов уязвимости.

Значения частично обобщенных показателей могут быть определены следующим образом. Пусть {К*} есть интересующее нас подмножество из полного множества потенциально возможных нарушителей.

Тогда вероятность нарушения защищенности информации указанным подмножеством нарушителей по *j*-му фактору в *i*-м компоненте АСОД - $P_{i\{K^*\}}^{(r)}$ - определится выражением:

$$P_{i\{K^*\}}^{(r)} = 1 - \prod_{\forall k^*} [1 - P_{ijk}^{(б)}] \qquad (4.7)$$

где $\forall k^*$ означает перемножение выражений в скобках для всех *k*, входящих в подмножество {К*}. При этом верхний индекс *r* будет принимать значение (ц), (п) или (р) в зависимости от того, какие базовые показатели используются при расчетах.

Аналогично, если $\{J^*\}$ есть подмножество представляющих интерес дестабилизирующих факторов, то уязвимость информации в *i*-м компоненте по данному подмножеству факторов относительно *k*-го нарушителя определится выражением:

$$P_{i\{J^*\}k}^{(r)} = 1 - \prod_{\forall j^*} \left[1 - P_{ijk}^{(б)} \right] \qquad (4.8)$$

Наконец, если {I*} есть подмножество интересующих нас структурных компонентов АСОД, то уязвимость информации в них по *j*-му фактору относительно *k*-го нарушителя

$$P^{\{I^*\}jk} = 1 - \prod_{\forall i} \left[1 - P^{ijk}\right]. \qquad (4.9)$$

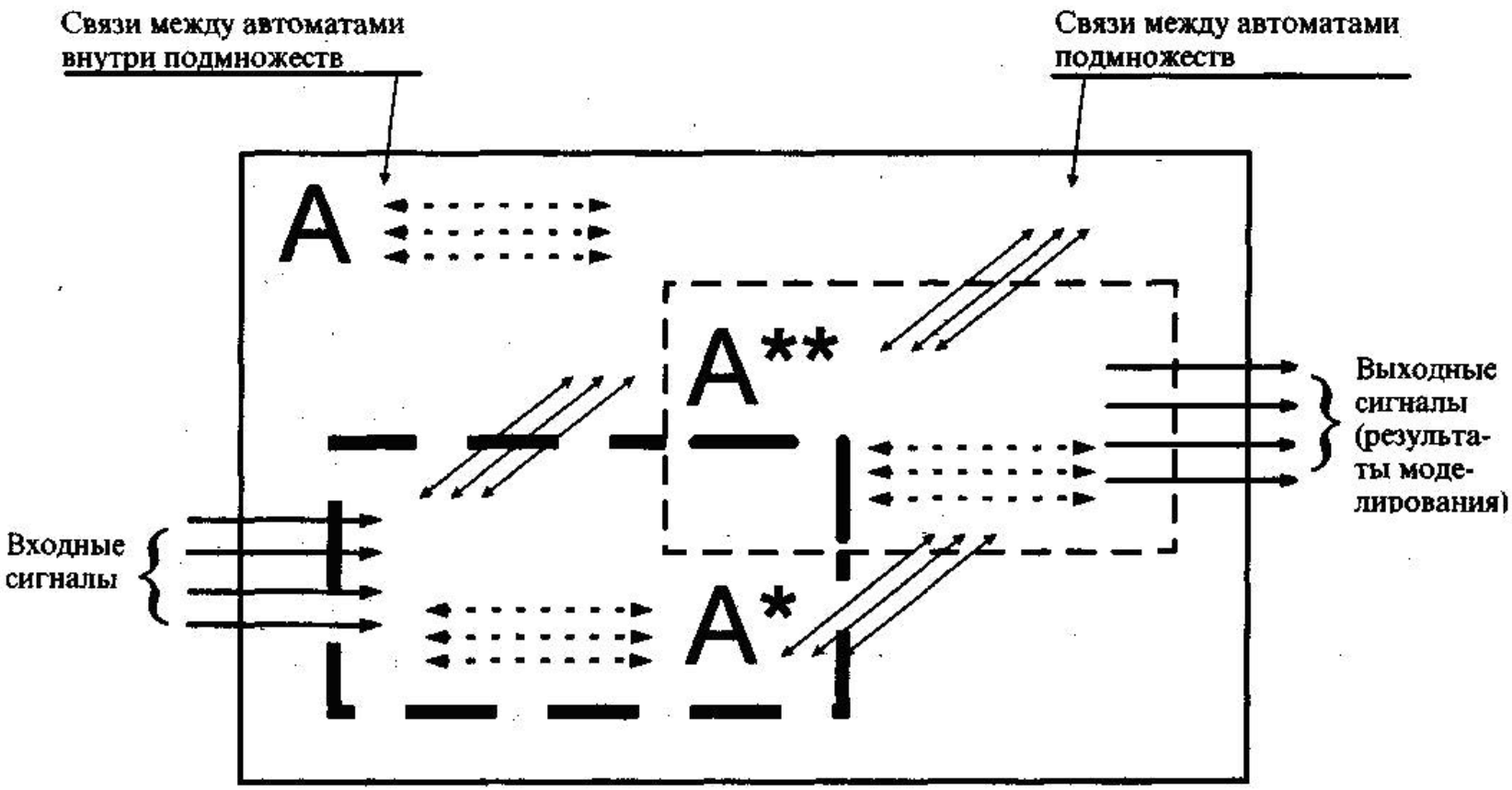

Связи между автоматами внутри подмножеств
Связи между автоматами подмножеств
A
A**
A*
Входные сигналы
Выходные сигналы (результаты моделирования)

Рисунок 4.7. – Общая структура вероятностно-автоматной модели АСОД

Каждое из приведенных выше выражений позволяет производить обобщение по одному какому-либо параметру. Нетрудно получить общее выражение. Так, если нас интересуют подмножества ***{I*}, {J*} и {K*}*** одновременно, то

$$P^{(r)}_{\{I^*\}\{J^*\}\{K^*\}} = 1 - \prod_{\forall i^*}[1 - P^{ijk}_{(б)}]\prod_{\forall j^*}[1 - P^{ijk}_{(б)}]\prod_{\forall k^*}[1 - P^{ijk}_{(б)}]. \quad (4.10)$$

Очевидно, общий показатель уязвимости $P^{(r)}$ определяется из выражения

$$P^{(r)} = 1 - \prod_{\forall i}[1 - P^{ijk}_{(б)}]\prod_{\forall j}[1 - P^{ijk}_{(б)}]\prod_{\forall k}[1 - P^{ijk}_{(б)}] \quad (4.11)$$

Выведем выражения для определения экстремальных показателей уязвимости. Экстремальными названы показатели, характеризующие наиболее неблагополучные условия защищенности информации: самый уязвимый структурный компонент АСОД - $\bar{i}$, самый опасный дестабилизирующий фактор - $\bar{j}$, самая опасная категория нарушителей - $\bar{k}$.

Тогда

$$\bar{i} = iEP^{(з)} \rightarrow \max \forall i. \quad (4.12)$$

Данное выражение читается так: $\bar{i}$ есть такое i, для которого заданный показатель уязвимости $P^{(з)}$ принимает максимальное значение для всех i.

Аналогично:

$$\bar{j} = iEP^{(з)} \rightarrow \max \forall j \quad (4.13)$$

$$\bar{k} = iEP^{(з)} \rightarrow \max \forall k \quad (4.14)$$

Рассмотрим далее методы расчета показателей уязвимости информации с учетом интервала времени, на котором оценивается уязвимость.

Нетрудно видеть, что приведенные выше выражения являются адекватными для таких интервалов времени, которые названы нами очень малыми. Для других интервалов полученные формулы не будут адекватными: чем больше интервал времени, тем больше возможностей у нарушителей для злоумышленных действий и тем больше вероятность

изменения состояния АСОД и условий автоматизированной обработки информации.

Возможные подходы к учету указанных факторов могут быть следующими. Напомним, что малыми мы называем такие временные интервалы, которые нельзя сводить к точке, но происходящие на которых процессы относительно уязвимости информации можно считать однородными. Тогда естественным будет разделить малый интервал на очень малые и на каждом из таких очень малых интервалов определять уязвимость информации независимо от других. А поскольку происходящие на малом интервале времени процессы являются однородными, то на каждом из выделенных очень малых интервалов уязвимость будет определяться по одной и той же зависимости. Тогда, если через $P(m)$ обозначить интересующий нас показатель уязвимости

в точке (на очень малом интервале), а через $P(\mu)$ - тот же показатель на

малом интервале, то

$$P(\mu) = 1 - \prod_{t=1}^{n} [1 - P(m)] \quad (4.15)$$

где t- переменный индекс очень малых интервалов, на которые поделен малый интервал; n - общее число таких интервалов.

t

Нетрудно видеть, что рассмотренный подход можно распространить и на другие интервалы, а именно: большой интервал представить некоторой последовательностью малых, очень большой - последовательстъю больших,

бесконечно большой - последовательностью очень больших.

Однако приведенные выражения будут справедливыми лишь в том случае, если на всем рассматриваемом интервале времени условия для нарушения защищенности информации остаются неизменными. В

действительности эти условия могут изменяться, причем наиболее важным фактором, влияющим на эти условия, является активное действие системы защиты информации. Технология функционирования системы защиты

специально будет рассматриваться в дальнейшем, однако чисто интуитивно можно предположить, что чем выше уязвимость информации, тем сильнее и

активнее должна воздействовать система защиты. Учитывая сказанное, можно записать

$$P^{(m)} = f\left[P^{(m)}(t-1)\right], \qquad (4.16)$$

т.е. значение точечного P показателя в каждой точке рассматриваемого интервала есть некоторая функция значения этого показателя в предыдущей точке. Тогда выражение (4.15) должно быть представлено так:

$$P^{(\mu)}_{t=1} = 1 - \prod_{t}^{n}\{1 - f[1 - P^{(m)}(t-1)]\}. \qquad (4.17)$$

Рассмотренные выше модели являются аналитическими, поскольку они позволяют определять требуемые значения показателей уязвимости путем аналитических вычислений.

Очень часто возникает необходимость в определении значений показателей уязвимости на конкретных технологических маршрутах автоматизированной обработки защищаемых данных. Рассмотрим возможные подходы к решению данной задачи. Технологические маршруты,

по которым может осуществляться обработка информации, могут иметь различную структуру. Однако в качестве типовых можно выделить такие маршруты: простой технологический; развитый (сложный), но хорошо структурированный; сложный неструктурированный;

Рассмотрим структуру и содержание аналитической модели определения показателей уязвимости информации для перечисленных вариантов схем.

Простой технологический маршрут обработки данных можно задать упорядоченной последовательностью номеров ТСК, участвующих в обработке, и их состояний $\{i_s, \theta_s^{(i)}\}$, где переменный индекс s означает порядковый номер компонента в последовательности, а $\theta_S^{(i)}$ - состояние его в соответствующий момент времени.

Данная последовательность формируется по следующим правилам:

1) ТСКупорядочиваютсявстрогомсоответствиис последовательностью их участия в обработке информации;

2) если продолжительность обработки информации на одном и том же ТСК в одном и том же состоянии превышает стандартный интервал времени

ΔT_{cm}, то он повторяется несколько раз с последовательно возрастающими значениями s;

3) если в течение ΔT_{cm} состояние ТСК изменяется, то s последовательно повторяется по числу состояний ТСК, причем s растет в соответствии с последовательностью смены состояний;

4) если на технологическом маршруте обработки данных встречаются циклы, то циклически повторяющиеся ТСК заключаются в прямоугольные скобки, причем снаружи вверху у закрывающей скобки указывается число повторений цикла или условие, определяющее это число;

5) если на технологическом маршруте встречаются разветвления, то они описываются следующим образом: производится идентификация всех ветвлений (например, арабскими цифрами), причем начальный и конечный узлы каждого разветвления обозначаются одним и тем же идентификатором;

все ТСК, входящие в одну и ту же ветвь, заключаются в фигурные скобки, причем снаружи вверху у открывающей и закрывающей скобок проставляется идентификатор ветви.

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Ознакомиться с графиком значений базовой вероятности нарушения физической целостности информации

3. Рассмотреть вероятностно-автоматную модель ТСК АСОД

4. Изучить укрупненную схему модели определения показателей уязвимости информации

5. Ознакомиться с общей структурой вероятностной модели АСОД

6. Оформить отчет.

Содержание отчета и его форма

Отчет должен иметь форму согласно оформлению простого реферата.

Титульный лист должен включать название дисциплины, название практической работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической работы должна содержать:

1. Описание общей модели процесса нарушения физической целостности информации

2. Описание обобщенной структуры имитационной модели

3. Описание вероятностно-автоматной модели ТСК АСОД

4. Описание укрупненной схемы модели определения показателей уязвимости информации

5. Выводы по проделанной работе.

Вопросы для защиты работы

1. Выведите формулу для определения базового показателя уязвимости информации

2. Раскройте принципы и приведите пример определения обобщенных показателей уязвимости.

Лабораторная работа № 5

ИССЛЕДОВАНИЕ ПОКАЗАТЕЛЕЙ УЯЗВИМОСТИ ИНФОРМАЦИИ ДЛЯ РАЗЛИЧНЫХ УЧАСТКОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Цель и содержание: провести исследование показателей уязвимости информации для различных участков технологического процесса

Теоретическое обоснование

Линейный участок. Пронумеруем все ТСК, образующие линейный участок технологического маршрута, последовательно возрастающими номерами $0,1,2,...,s,...,n$.

Обозначим через $P^{0\,(вх)}$ вероятность того, что на вход ТСК с номером 0 поступает информация с нарушенной защищенностью, а через P_S вероятность того, что такое нарушение будет иметь место в выходной информации ТСК, соответствующего s-му номеру.

Поскольку выходная информация ТСК, соответствующего номеру s, то очевидно, справедливыми будут следующие соотношения:

$$P = 1 - [1 - P^{(вх)}](1 - P'); \quad (1)$$

$$P_S = 1 - [1 - P_{S-1}](1 - P'_S)$$

$s = 1,2,...,n,$

где P^0 и P^S - вероятности того, что защищенность информации будет нарушена в процессе прохождения ее в соответствующем ТСК.

Циклический участок. Показатели уязвимости информации для циклического технологического процесса могут быть определены по тем же зависимостям, что и для линейного участка, поскольку циклический участок

может быть трансформирован в повторяющийся необходимое число раз линейный. Иными словами, циклическую процедуру можно представить матрицей (рисунок 1).

Матрицу затем можно представить в виде линейной последовательности:

$10,11,...1s,...,1n,20,21,...,2s,...,2n,...q0, q1,...qs,...qn,..., m0, m1,..., ms,..., mn.$

После этого можно использовать приведенные выше зависимости для линейного маршрута.

Ветвящийся участок. В модели определения показателей уязвимости информации для ветвящегося участка выделяются три вопроса: определение показателей уязвимости информации на входах каждой из ветвей ветвящегося процесса; определение показателей уязвимости информации в ТСК, составляющих каждую из ветвей ветвящегося процесса; определение показателей уязвимости информации на входе того ТСК, на котором заканчивается несколько ветвей ветвящегося процесса.

Ответ на первый вопрос, очевидно, заключается в том, что показатели уязвимости на входе каждой из ветвей ветвящегося процесса будут равны показателям уязвимости на выходе того ТСК, после которого начинается разветвление, т.е. $\forall q \in b$ (b - количество ветвей в ветвящемся процессе):

а

Последовательность повторений цикл

Повторяющийся линейный участок Технологического процесса

	1	2	3 · · · *s*	· · · *n*
1	10 11	12 · · · 1*s*	· · · 1*n*	
2	20	21	22	· · · 2*s*	· · · 2*n*
.	.	.	. .	.
.	.	.	. .	.
.	.	.	. .	.
q	*q*0	*q*1	*q*2	· · · *qs*	· · · *qn*
.	.	.	. .	.
.	.	.	. .	.
.	.	.	. .	.
m	*m*0	*m*1	*m*2	· · · *ms*	· · · *mn*

Рисунок 1 – Схематическое представление циклического участка

$$P_{q0}^{(в\,х)} = P_i' \qquad (2)$$

где *i*-индекс того ТСК, с которого начинается развитие.

Значение показателей уязвимости информации в ТСК каждой из ветвей ветвящегося процесса (второй вопрос) могут быть определены по тем же зависимостям, что и для линейного участка, с учѐтом сказанного выше относительно значений показателей уязвимости информации на входе первого ТСК ветви.

Несколько сложнее ответить на третий вопрос, т.е. определить значение показателей уязвимости информации на входе того ТСК, на котором заканчивается несколько ветвей ветвящегося процесса. На рисунке 2

приведена схема такого окончания ветвящегося процесса. Очевидно, здесь возможны три случая: 1) каждый раз выполняется одна какая-либо ветвь; 2) каждый раз выполняется несколько ветвей, причем перечень и число их заранее неизвестно; 3) каждый раз обязательно выполняются все ветви процесса.

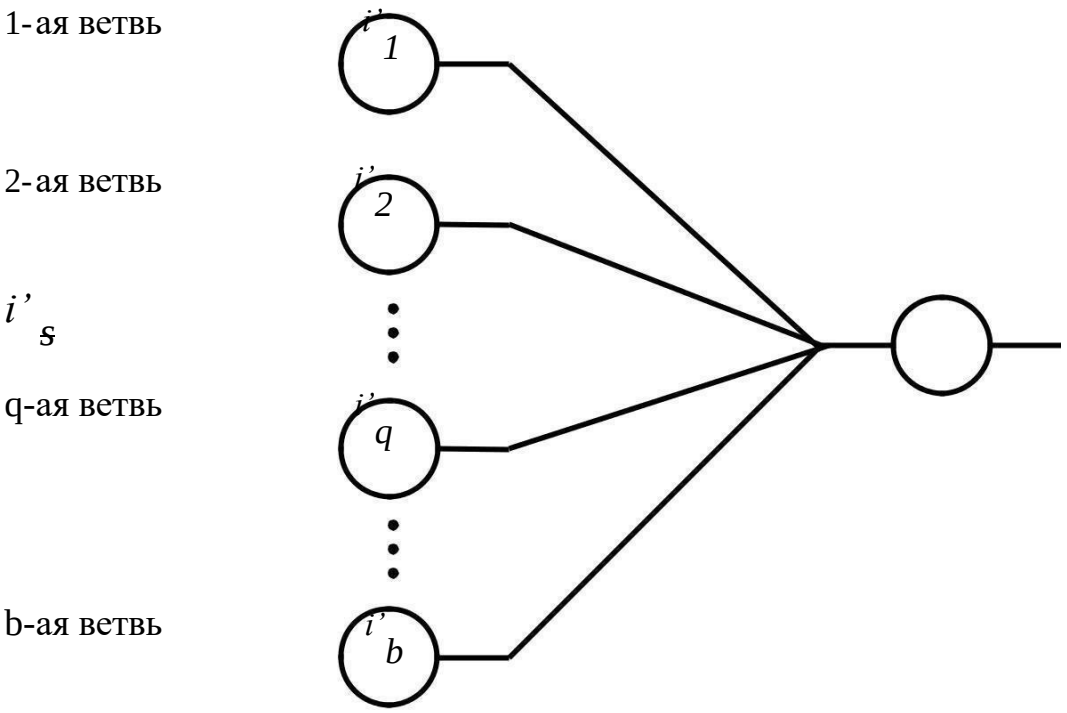


Рисунок 2 – Схема окончания ветвящегося процесса

В первом случае, если имеется возможность определить, какая из ветвей выполняется (q), то очевидно, для ТСК с индексом i^s

$$P_{i_s}^{(вх)} = P_{i_q}' \tag{3}$$

Если же номер исполняется ветви не может быть определен, то

$$P_{i_s}^{(вх)} = P_i' \tag{4}$$

с вероятностью $P(q)$, где $P(q)$ есть вероятность того, что используется q-я ветвь.

Второй случай носит наиболее общий характер, в этом случае:

$$i_S^{(вх)} = 1 - \prod_{\forall q} \left(1 - P_{i_q}^{(вых)}\right)^{P(q)}. \tag{5}$$

Наконец, в третьем случае

$$= 1 - \prod_{\forall q \in h_q} \left(1 - P^i\right), \quad (6)$$

т.е. в (5) $P^{(q)}_q = 1$ для всех q.

Развитой структурированной технологической схемой обработки информации названа такая схема, которая может быть разложена на несколько простых маршрутов. Отсюда следует, что в этом случае по рассмотренным выше зависимостям могут быть определены показатели уязвимости для каждого из составляющих маршрутов, а затем полученные данные могут быть синтезированы применительно к исходной технологической схеме.

Рассмотрим теперь сложные режимы функционирования системы обработки. Характерной особенностью сложных слабоструктурированных схем обработки является невозможность разделения и на некоторую совокупность вполне определенных маршрутов, вследствие чего рассмотренные выше модели определения показателей уязвимости не могут быть использованы. В этих условиях можно перейти к обобщенным средневзвешенным параметрам, т.е. воспользоваться зависимостями.

Подводя итоги изложенному выше, следует отметить, что использование аналитических моделей для определения показателей уязвимости информации на технологических маршрутах обработки сопряжено со значительными трудностями. Во многих случаях более эффективными будут статистические модели, причем технологический маршрут удобно представить в виде совокупности взаимосвязанных вероятностных автоматов, каждый из которых имитирует работу соответствующего ТСК, а направленность взаимосвязей автоматов соответствует технологическому маршруту обработки информации.

Далее для реализации концепции управления защитой информации необходимо иметь средства и методы прогнозирования значений показателей уязвимости информации.

Прогнозирование показателей уязвимости информации заключается в предсказании ожидаемых их значений на заданный период упреждения.

Необходимость такого прогнозирования возникает в процессе решения всех основных задач управления защитой и особенно задач планирования и

оперативно-диспетчерского управления. При решении задач планирования необходимы ожидаемые значения показателей уязвимости в различные моменты времени планируемого периода. При этом, если планирование осуществляется с учетом опыта управления защитой информации в предшествующие периоды времени, то значения показателей определяются путем прогнозирования на основе значений по данным предыстории.

Принятие же решений в процессе оперативно-диспетчерского управления защитой информации полностью базируется на прогнозе значения показателей.

Нетрудно показать, что изменение значений показателей уязвимости во времени в процессе функционирования системы обработки представляет собой случайный процесс, поэтому и задача прогнозирования значений этих показателей сводится к задаче предсказания случайных процессов. В теории случайных процессов известно несколько методов решения этой задачи:

экстраполяция случайных функций, построения автокорреляционной функции, эволюционного моделирования и некоторые другие.

С целью упрощения методов решения рассматриваемой задачи представляется целесообразным воспользоваться рассмотренными особенностями зависимостей показателей качества информации от параметров системы обработки при различный вариантах технологического процесса обработки информации. Как и в случае определения текущих значений показателей уязвимости, будем различать следующие варианты технологического процесса: простой технологический маршрут обработки информации; развитая структурированная схема функционирования системы обработки; сложная слабоструктурированная схема функционирования системы обработки.

Простым технологическим маршрутом нами названа такая технологическая схема обработки информации, которую однозначно можно представить упорядоченной последовательностью пар $\{i_s, \theta_s^{(i)}\}$, где i_s – номер

ТСК, участвующего в обработке информации на s-м месте в общей очередности; $\theta_s^{(i)}$ – состояние i-го ТСК в этот момент времени.

Поскольку технологический процесс обработки информации может быть представлен с такой степенью однозначности, то на любой момент времени можно определить не только состояние системы обработки информации, но и последовательную смену состояний на анализируемом промежутке времени. Благодаря такой однозначности, прогнозирование значение показателей качества информации может быть осуществлено по зависимостям, приведенным выше при определении значений показателей уязвимости на технологических маршрутах.

К развитым структурированным схемам функционирования систем обработки отнесены такие схемы, которые можно расчленить на некоторое количество простых технологических маршрутов обработки, и к прогнозированию показателей уязвимости информации можно подойти аналогично тому, как и выше, а именно: расчленить сложную схему на составляющие маршруты, рассчитать прогнозные значения показателей уязвимости для каждого такого маршрута, затем рассчитать интересующие обобщенные показатели.

Однако, если система обработки функционирует продолжительное время в структурированном режиме, то появляются объективные возможности собрать опытные данные по защищенности информации. Эти данные удобно представить в виде матрицы $| \xi^{iz}, j^{iz}, \theta^{iz} |$, гед

$$\begin{cases} 1, & \text{если в } i \text{ - м ТСК на } z \text{ - м интервале времени имело место } \xi_{iz} = \\ & \text{нарушение защищенности;} \\ 0, & \text{в противном случае;} \end{cases}$$

j_{iz} – номер дестабилизирующего фактора, проявление которого явилось причиной нарушения защищенности информации; θ_{iz} – индекс (номер)

типового состояния i -го ТСК на z -м интервале.

Имея эти данные и зная совокупность технологических маршрутов обработки информации в прогнозируемый период времени, с помощью известных методов экстраполяции случайные функций можно определить ожидаемые значения показателей уязвимости информации.

Для сложных слабоструктурированных технологических схем функционирования систем обработки наиболее адекватным методом прогнозирования показателей уязвимости будет статистическое моделирование. Однако ля того чтобы статистическим путем непосредственно прогнозировать значение показателей уязвимости необходимы многопараметрические статистические данные предыстории. В

настоящее время такие данные практически отсутствуют и получение их представляет собой весьма сложную проблему.

С целью упрощения задачи будем прогнозировать не непосредственные показатели уязвимости, а составляющие величины,

входящие в выражение для этих показателей. Как следует из моделей оценки показателей уязвимости, таким величинами являются вероятности: 1)

проявления дестабилизирующих факторов; 2) наличия информации в месте и во время проявления дестабилизирующих факторов; 3) нарушения защищенности информации под воздействие дестабилизирующих факторов,

несмотря на применение средств защиты.

Рассмотрим возможные подходы к
прогнозированию перечисленных величин.

Вероятность проявления дестабилизирующих факторов $P_{ij\theta}$. При

установившемся процессе функционирования системы обработки проявление дестабилизирующих факторов можно считать случайным пуассоновским

процессом. Если через $\lambda_{ij\theta}$ обозначить интенсивность потока *j*–го фактора в *i*-

м ТСК, находящемся в θ-м состоянии, то в соответствии со свойствами пуассоновского процесса

$$P_{ij\theta} = \lambda_{ij\theta} \cdot \delta t \quad (7)$$

где δt – интервал времени, существенно меньший того интервала, относительно которого определено значение $\lambda_{ij\theta}$. Поскольку для общего случая интервал прогнозирования этому условию не будет удовлетворять $P_{ij\theta}$

выразим следующим образом:

$$P_{ij\theta} = 1 - (1 - \lambda_{ij\theta})^{F\ \Delta t} \quad (8)$$

где t – интервал прогнозирования. ***защищаемой информации*** $P_i^{(u)}$.

Вероятность наличия в ТСК

Разделим весь период прогнозирования t на маленькие интервалы продолжительностью δt и через z обозначим текущий порядковый номер (относительно начального момента) такого интервала.

Положим

$$\gamma_{iz} = \begin{cases} 1, \text{ если в } i\text{-м ТСК на } z\text{-м интервале назходится в активном рабочем состоянии;} \\ 0, \text{ в противном случае;} \end{cases}$$

Тогда при условии $t >> \delta t$ d качестве вероятности $P_i^{(u)}$ можно принять

$$P_{(u)}^{i} = \frac{\sum_z \gamma_{iz}}{\frac{\Delta t}{\delta t}} = \frac{\frac{\Delta t}{\delta t} \sum_z \gamma_{iz}}{z} \quad (9)$$

Значения функции γ_i могут быть определены по технологическому графику обработки информации в прогнозируемый период времени.

Вероятность нарушения защищенности информации в i-м ТСК по j-

P
му фактору $_{ij}^{(н)}$. Разделим период прогнозирования на маленькие интервалы времени δ_z и рассмотрим функцию

$x^{i\eta\ z}$ = { 1, если η - е средство защиты на z − м интервале активно используется в i - м ТСК; 0, в противном случае.

Если через $P^{ij}(\eta)$ обозначить вероятность того, что при использовании η -го средства в i -го ТСК нарушение защищенности информации при проявлении j -го дестабилизирующего фактора не будет иметь места, то при $\Delta t >> \delta t$ значение $P(u)^{ij}$ можно определить следующим образом:

$$P_{ij}(u) = \prod_{\forall \eta} (1 - P^{ij}(\eta) \frac{\Delta t}{\delta t} \sum_{z} X^{z\ i\eta}). \qquad (10)$$

Однако, как уже отмечалось выше, прогнозирование случайных процессов является слабоструктурированной задачей, поэтому методы прогнозирования, приемлемые по сложности и трудоемкости, могут не обеспечить приемлемую точность прогноза. С целью повышения точности прогноза (особенно при использовании упрощенных методик прогнозирования) целесообразно предусмотреть процедуру перманентной корректировки алгоритма прогнозирования с целью непрерывного его совершенствования. Постановка данной задачи может быть сформулирована следующим образом. Пусть (рис. 3) в момент времени t_1 был произведен прогноз показателя уязвимости информации на глубину от t_1 до t_2.

Прогнозные значения показателя на рисунке показаны пунктирной линией. Пусть по достижении момента времени t_2 действительные значения данного показателя оказались такими, как показано на рисунке сплошной линией $П_p(t)$.

Если через A_1 обозначить алгоритм прогнозирования,

использовавшийся в момент времени t_1, а через A_2 – скорректированный алгоритм, который целесообразно использовать в момент времени t_2, то

$$A = F \left[A_1; \int_{t_1}^{t_2} | \Pi_n(t/A) - \Pi_{1p}(t) | dt \right], \qquad (11)$$

причем A_2 должно быть таким, чтобы

$$\Delta\Pi = \int_{t_1}^{t_2} | \Pi_n(t/A)_{2p} - \Pi(t) dt \qquad (12)$$

было минимальным.

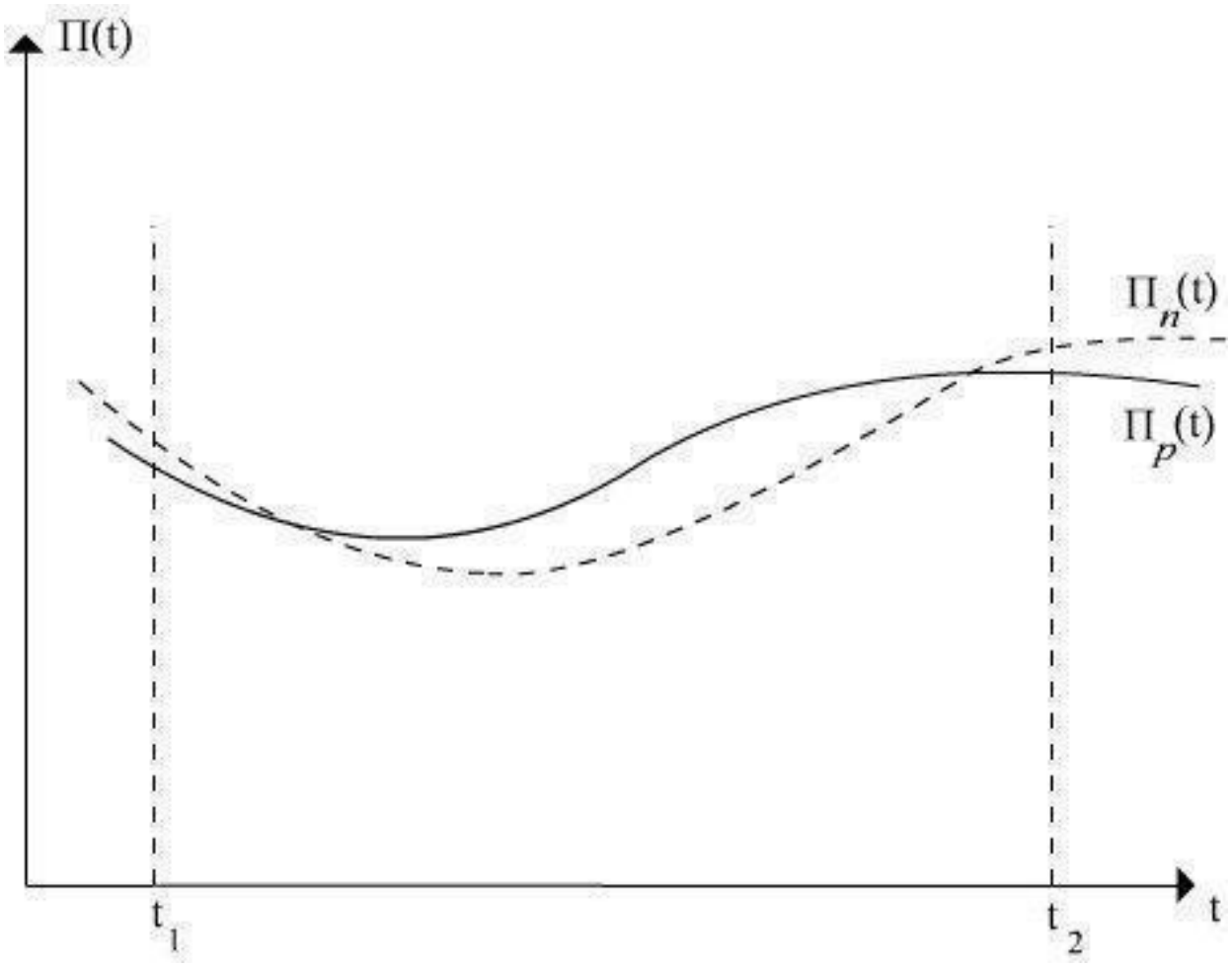


Рисунок 3 – Иллюстрация к постановке задачи корректировки алгоритма прогнозирования значений показателей уязвимости информации.

Здесь $П^{n}(t/A^{1})$ и $П_{n}(t/A_{2})$ – прогнозные значения показателя уязвимости при использовании алгоритмов A_1 и A_2.

Рекомендации по использованию моделей оценки уязвимости информации

Рассмотренные в предыдущих параграфах модели позволяют определять текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов АСОД, любой их комбинации и для любых условий жизнедеятельности АСОД. Иными словами, предложенный комплекс моделей является полным в том смысле,

что он обеспечивает решение практически всех задач анализа и синтеза систем защиты и управления процессами ее функционирования.

Относительно адекватности моделей тем реальным процессам, для имитации которых они предназначаются, следует сделать два существенных замечания: 1) практически все модели построены в предположении независимости тех случайных событий, совокупности которых образуют сложные процессы защиты информации в современных АСОД; 2) для обеспечения работы моделей необходимы большие объемы таких исходных данных, подавляющее большинство которых в настоящее время отсутствует,

а формирование их сопряжено с большими трудностями.

Рассмотрим коротко существо приведенных замечаний и определим порядок использования моделей в этих условиях.

Замечание первое – допущение независимости случайных событий,

происходящих в системах защиты информации. Основными событиями,

имитируемыми в моделях определения показателей уязвимости, являются:

проявление дестабилизирующих факторов на защищаемую информацию и воздействие используемых средств защиты на дестабилизирующие факторы.

При этом сделаны следующие допущения (причем в аналитических – в явном виде):

1) потенциальные возможности проявления каждого дестабилизирующего фактора не зависят от проявления других;

2) каждый из злоумышленников действует независимо от других, т.е. не учитываются возможности формирования коалиции злоумышленников;

3) негативное воздействие на информацию каждого из проявившихся дестабилизирующих факторов не зависят от такого же воздействия других проявившихся факторов;

4) негативное воздействие дестабилизирующих факторов на информацию в одном каком-либо компоненте АСОД может привести лишь к поступлению на выходы связанных с ним компонентов информации с нарушенной защищенностью и не оказывает влияния на такое же воздействие на информацию в самих этих компонентах;

5) каждое из используемых средств защиты оказывает нейтрализующее воздействие на дестабилизирующие факторы и восстанавливающее воздействие на информацию независимо от такого же воздействия других;

6) благоприятное воздействие средств защиты в одном компоненте АСОД лишь снижает вероятность поступления на входы связанных с ним компонентов информации с нарушенной защищенностью и не влияет на уровень защищенности информации в самих этих компонентах.

В действительности же события, перечисленные выше, являются зависимыми, хотя степень зависимости различна: от незначительной,

которой вполне можно пренебречь, до существенной, которую следует учитывать. Однако для решения данной задачи в настоящее время нет необходимых предпосылок, поэтому остаются лишь методы экспертных оценок.

Второе замечание касается обеспечения моделей необходимыми исходными данными. Выше уже неоднократно отмечалось, что для практического

использования моделей определения показателей уязвимости необходимы большие объемы разнообразных данных, причем подавляющее большинство из них в настоящее время отсутствует.

Сформулируем теперь рекомендации по использованию моделей, разработанных в рамках рассмотренных выше допущений, имея в виду, что это использование, обеспечивая решение задач анализа, синтеза и управления в системах защиты информации, не должно приводить к существенным погрешностям.

Первая и основная рекомендация сводится к тому, что моделями должны пользоваться квалифицированные специалисты-профессионалы в области защиты информации, которые могли бы в каждой конкретной ситуации выбрать наиболее эффективную модель и критически оценить степень адекватности получаемых решений.

Вторая рекомендация заключается в том, что модели надо использовать не просто для получения конкретных значений показателей уязвимости, а для оценки поведения этих значений при варьировании существенно значимыми исходными данными в возможных диапазонах их изменений. В этом плане модели, определения значений показателей уязвимости могут служить весьма ценным инструментом при проведении деловых игр по защите информации.

Третья рекомендация сводится к тому, что для оценки адекватности моделей, исходных данных и получаемых решений надо возможно шире привлекать квалифицированных и опытных экспертов.

Наконец, четвертая рекомендация заключается в том, что для эффективного использования моделей надо непрерывно проявлять повышенную заботу об исходных данных, необходимых для обеспечения моделей при решения задач защиты. Существенно важным при этом является то обстоятельство,

что подавляющее количество исходных данных обладает высокой степенью неопределенности. Поэтому надо не просто формировать необходимые данные, а перманентно их и оценивать и уточнять.

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Изучить формулы для определения показателей уязвимости информации на технологических маршрутах обработки информации

3. Изучить формулы для определения уязвимости информации на продолжительном интервале времени

4. Ознакомиться с рекомендациями по использованию моделей оценки уязвимости информации

5. Оформить отчет

Содержание отчета и его форма

Отчет должен иметь форму согласно оформлению простого реферата.

Титульный лист должен включать название дисциплины, название практической работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической работы должна содержать:

5. Формулы для определения показателей уязвимости информации на технологических маршрутах обработки информации

6. Формулы для определения уязвимости информации на продолжительном интервале времени

7. Описание подходов к прогнозированию значений показателей уязвимости информации

8. Основные рекомендации по использованию оценки угроз

9. Выводы по проделанной работе.

Вопросы для защиты работы

4. Выведите формулы для определения показателей уязвимости информации на технологических маршрутах обработки информации.

5. Выведите формулы для определения уязвимости информации на продолжительном интервале времени

6. Охарактеризуйте подходы к прогнозированию значений показателей уязвимости информации

7. В чем заключаются основные рекомендации по использованию оценки угроз.

Лабораторная работа № 6

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 пока-

зателей 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.

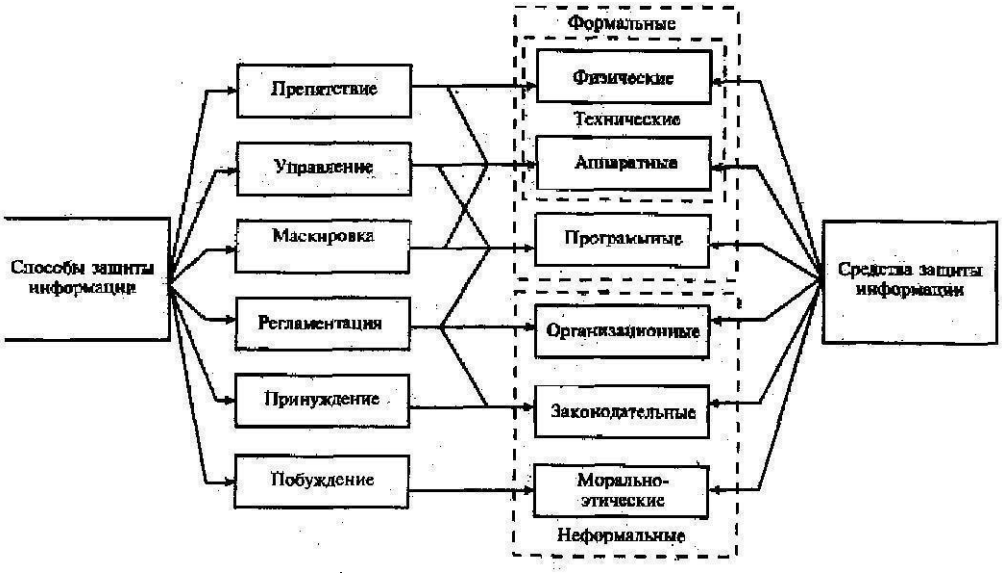


Рисунок 1 – Классификация способов и средств защиты информации

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

5.

6. мотивами)
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
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.

Таблица 1 – 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	1. Необходимость использований людей 2. Повышенная зависимости субъективных факторов 3. Высокая

		3. Подверженность случайным или	зависимость от общей организации робот на

закономерным объек определенные типы Э	е модификациям 4 ВМ	Ориентация на вполне	

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	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	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

	терминальных устройств 9 Установка . дополнительных	программ обеспечения процессов обработки	процедур и схем обеспечения обработки информации

средств выдачи данных 10. Создание дополнительного запаса сменных носителей информации 11 . Создание дополнительных ЗИ 12. Установка дополнительной контрольной и другой обеспечивающей аппаратуры 13. Создание дополнительных систем охраны и наблюдения			
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	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,	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

	технических средств, перечисленных в 1 3. Разработка технические средств включения в работу резервного устройства	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	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	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	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

	5. Оснащение	процедуры	людей и элементов

	дверей помещений и устройств АСОД радиоуправляемым и 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	опознавания 5. Программы проверки прав на доступ к ресурсам АСОД	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,	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

		по матрице	

		полномочий, по мандату 4. Программная реализация мандатной архитектуры ЗУ	
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	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)	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

	технических	5. Программы	данных, подготовки

	средств АСОД: по четности, методами специального кодирования, методами повторного выполнения операций, методами параллельного выполнения операций 4. Аппаратура измерение параметров внешней среды	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	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	1. Система правил регистрации данных, относящихся к защите информации 2. Ручное ведение регистрационных журналов

		5. Программы	

		регистрации проявлений дестабилизирующих факторов 6. Программы регистрации данных о нарушении зашиты информации	
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 практической работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической 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

Лабораторная работа № 7

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ТЕХНИЧЕСКИХ И ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ

Цель и содержание: провести исследование особенностей технических и программных средств защиты

Теоретическое обоснование

Технические средства защиты

Техническими, названы такие средства защиты, в которых основная защитная функция реализуется некоторым техническим устройством

(комплексом, системой). К настоящему времени разработано значительное количество различных технических средств, что дает достаточные основания для некоторых обобщенных их оценок.

К несомненным достоинствам технических средств относятся: достаточно широкий круг решаемых задач; достаточно высокая надежность;

возможность создания развитых комплексны, систем защиты; гибкое реагирование па попытки несанкционированных действии; традиционность используемых методов осуществления защитных функций.

Основные недостатки: высокая стоимость многих средств; необходимость регулярного проведения регламентных работ и контроля;

возможность додачи ложных тревог.

Системную классификацию технических средств удобно произвести по следующей совокупности критериев (см. рис. 6.3): сопряженность с основными средствами АСОД; выполняемая функция защиты; степень сложности устройства.

Структуризация значения критериев интерпретируется следующим образом.

Сопряженность с основными средствами АСОД: автономные средства; выполняющие свои защитные функций независимо от функционирования средств АСОД, т, е. полностью автономно; *сопряженные-*

средства, выполненные в виде самостоятельных устройств, но осуществляющие защитные функции в сопряжении (совместно) с основными средствами; *встроенные* - средства, которые конструктивно включены в состав аппаратуры технических средств АСОД,

Выполняемая функция защиты: внешняя защита - защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД; *опознавание* - специфическая группа средств,

предназначенных для опознавания людей но различным индивидуальным характеристикам; *внутренняя зашита* - зашита от воздействия дестабилизирующих, факторов, проявляющихся непосредственно в средствах обработки информации.

Степень сложности устройствами простые устройства - несложные приборы и приспособления, выполняющие отдельные процедуры защиты;

сложные устройства - комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты; *системы* - законченные технические комплексы,

способные осуществлять некоторую комбинированную процедуру защиты имеющую самостоятельное значение.

Если каждый элемент изображенной на рисунке 3 классификационной структуры представить в качестве группы технических средств защиты, то полный арсенал этих средств будет включать 27 относительно самостоятельных трупп.

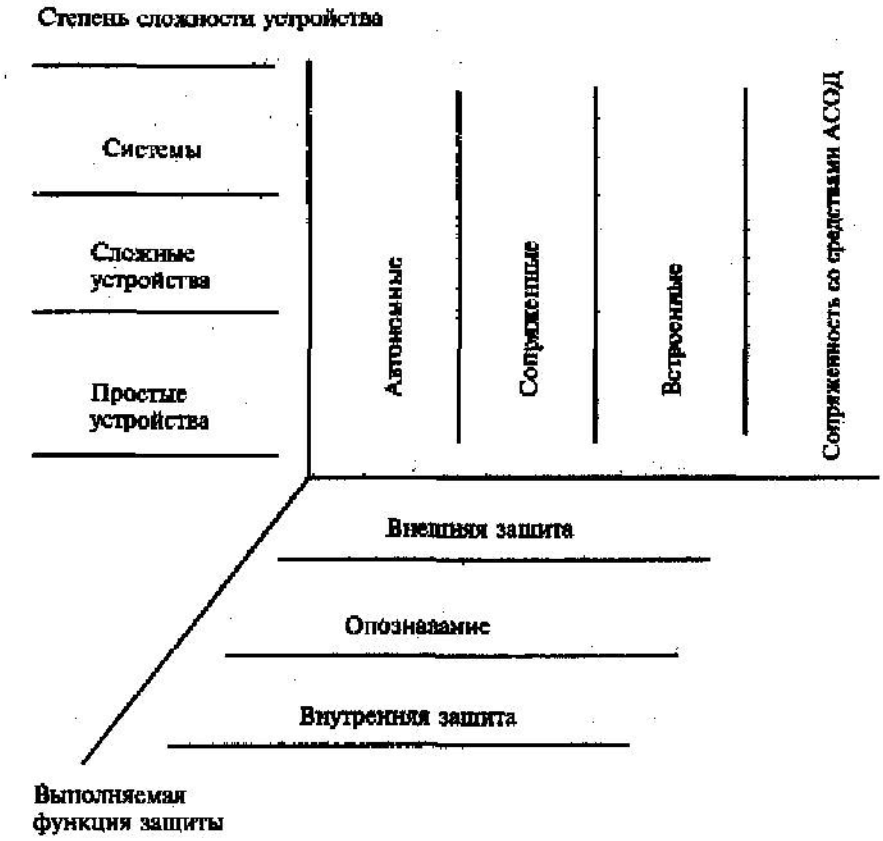


Рисунок 3 – Классификация технических средств защиты Нетрудно видеть, что в приведенной классификационной структуре

определяющей (в функциональном отношении) является классификация по критерию выполняемой функции; классификация же по критериям сопряженности и степени сложности отражает, главным образом,

особенности конструктивной и организационной реализации средств.

Поскольку для наших целей наиболее важной является именно функциональная классификация, то под данным углом зрения и рассмотрим технические средства защиты.

На рисунке 3 выведены три выполняемые техническими средствами макрофункции защиты: внешняя защита, опознавание и внутренняя защита.

Дальнейшая детализация функциональной классификации рассматриваемых средств приведена на рисунке 4. В каждой из 12 выделенных по функциональному признаку групп могут быть средства различной сложности и различного исполнения. К настоящему времени разработано большое

количество различных технических средств зашиты, причем налажено промышленное производство многих из них.

Ниже приводится описание некоторых типовых и широко используемых технических средств защиты.

Технически средств охранной сигнализации. Названные средства предназначаются для обнаружения угроз и для оповещения сотрудников охраны или персонала объекта о появлении и нарастании угроз. Охранная сигнализация по своему построению и применяемой аппаратуре имеет много общего с пожарной сигнализацией, поэтому они обычно объединяются в единую систему охранно-пожарной сигнализации (ОГТС).

Важнейшими элементами ОПС являются датчики; их характеристики определяют основные параметры всей системы.

По своему функциональному назначению эти датчики подразделяются на следующие типы:

1) *объемные,* позволяющие контролировать пространство помещений;

2) *линейные* или поверхностные для контроля периметров территорий и зданий;

3) *локальные* или точечные для контроля отдельных предметов.

Датчики могут устанавливаться как открыто, так и скрытно. Скрытно установленные датчики монтируются в почву или ее покрытие, под поверхности стен, строительных конструкций и т. п.

Наибольшее распространение получили следующие типы датчиков:

1) *выключатели и размыкатели,* действующие по принципу механического или магнитного управления размыканием электрической цепи при появлении нарушителя;

2) *инфраструктурные,* устанавливаемые на металлических ограждениях и улавливающие низкочастотные звуковые колебания ограждений во время их преодоления;

3) *электрического поля,* состоящие из излучателя и нескольких приемников, и излучатель, и приемники выполняются из электрических

кабелей, натянутых между столбами. При появлении нарушителя между излучателем и приемником между ними изменяется электрическое поле,

которое и фиксируется датчиком;

4) *инфракрасные*, действующие по тому же принципу, что и датчики электрического поля, в качестве излучателей используются инфракрасные светодиоды или небольшие лазерные установки;

5) *микроволновые*, состоящие из сверхвысокочастотных передатчика де, приемника. При попытке прохода, между передатчиком и приемником изменяется электромагнитное поле, которое и регистрируется приемником;

6) *давления,* реагирующие на механические нагрузки на среду, в которую они уложены;

7) *магнитные,* изготавливаемые в виде металлической сетки и реагирующие на металлические предметы, имеющиеся у нарушителя;

Рисунок 4 – Классификация технических средств защиты по функциональному назначению

8) *ультразвуковые,* реагирующие на ультразвуковые волны, возникающие при воздействии нарушителя на элементы конструкции охраняемого объекта;

9) *емкостные,* реагирующие на изменения электрической емкости между полом помещения и решетчатым внутренним ограждением.

Средства оповещение и связи. В качестве таких средств используются сирены, звонки и лампы, подающие достоянные или прерывистые сигналы о

том, что датчик зафиксировал появление угрозы. Радиосвязь дополняет тревожное оповещение и дает возможность уточнить характер угрозы и ее размеры.

Каналами связи в системе охранной сигнализации могут быть специально проложенные проводные линии, телефонные линии объекта,

телеграфные линии и радиосвязь.

Наиболее распространенные каналы связи многожильные экранированные кабели, которые для повышения надежности и безопасности работы сигнализации помещают в металлические или пластмассовые трубы или металлорукава.

Энергоснабжение системы охранной сигнализации должно осязательно резервироваться. Тогда в случае выхода его из строя функционирование сигнализации не прекращается за счет автоматического подключения резервного (аварийного) энергоисточника.

Охранное телевидение. Телевидение относится к одному из наиболее распространенных технических средств защиты. Главные достоинства охранного телевидения - возможность не только фиксировать факт нарушения режима охраны объекта, но и контролировать обстановку вокруг объекта, обнаруживать причины срабатывания охранной сигнализации, вести скрытое наблюдение и производства видеозапись охраняемого места или предмета, фиксирую действия нарушителя.

В отличие от обычного телевидения, в системе охранного телевидения монитор принимает только определенное изображение от одной или нескольких видеокамер, установленных в известном только ограниченному кругу лиц месте. Кроме сотрудников службы охраны никто не может наблюдать эти изображения, поэтому такую систему называют закрытой.

Классическая (и простейшая) схема организации охранного телевидения представляет собой несколько камер, каждая из которых соединена кабельной линией со своим монитором, находящимся в помещении поста охраны.

Камера является наиболее важным элементом системы охранного, телевидения. В настоящее время разработано и выпускается большое

количество разнообразных типов и моделей камер: видиконовые, сверхвысокочувствительные, с инфракрасной подсветкой и др.

Обязательной составной частью комплексной системы защиты любого вида объектов является *охранное освещение.* Различают два вида охранного освещения - дежурное (или постоянное) и тревожное.

Дежурное освещение предназначается для постоянного, непрерывного использования во внерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри зданий. Дежурное освещение оборудуется с расчетом его равномерности по всему пространству охраняемых зон объекта.

Для дежурного охранного освещения используются обычные, уличные

(вне здания) и потолочные (внутри здания) светильники. На посту охраны объекта должен находится силовой рубильник включения внешнего дежурного освещения или устройство автоматического включения внешнего освещения с наступлением темного временя суток.

Тревожное освещение включается сотрудниками охраны вручную или автоматически при поступлении сигнала тревоги от системы сигнализации.

Если тревожное освещение располагается по периметру территории, то по сигналу тревоги могут включаться светильники либо только в том месте,

откуда поступил сигнал тревоги, либо по всему периметру территории.

Для тревожного освещения обычно используют прожектор большой мощности или несколько прожекторов средней мощности до 1000 Вт.

Так же, как и сигнализация, дежурное освещение должно иметь резервное электропитание на случай аварии или выключения электросети.

Наиболее распространенный способ резервирования дежурного освещения -

установка светильников, имеющих собственные аккумуляторы. Такие светильники постоянно подключены к электросети (для подзарядки аккумуляторов), а в случае ее аварии автоматически включаются от собственного аккумулятора.

Рассмотренные выше средства относятся к категории средств обнаружения угрозы. Самостоятельную категорию составляют средства противодействия возникновению и распространению угроз. Сюда относятся естественные и искусственные барьеры (водные преграды,

сильнопересеченная местность, заборы, ограждения из колючей проволоки и т. п.), особые конструкции помещений, сейфы и др.

В качестве иллюстрации приведен краткое описание одной из новейших систем охранно-пожарной сигнализации, разработанной отечественной фирмой МИККОМ и известной под названием МИККОМ

AS101. Данная система представляет собой компьютеризованную автономную систему и предназначена для защиты от несанкционированного доступа в производственные и служебные помещения защищаемых объектов.

Она является новым поколением изделий подобного назначения и отличается расширенными функциональными возможностями: управление работой системы может осуществлять с периферийных кодовых устройств с помощью индивидуальных электронных карточек пользователей,

предусмотрено графическое отображение плана объекта, обеспечиваются повышенные сервисные возможности протоколов и баз данных системы.

Значительно повышена надежность системы.

Возможности системы позволяют одновременно выполнять функции охранной системы и системы доступа. В отличие от большинства зарубежных аналогов постановка и снятие с охраны зон объекта может осуществляться не по установленным временным интервалам, а

пользователями непосредственно с периферийных устройств.

Система обеспечивает выполнение следующих функций:

1) автоматическую выдачу сообщений о несанкционированных попытках проникновения в охраняемые объекты, попытках хищений из шкафов и сейфов, оборудованных датчиками охранной сигнализации,

возгораниях в помещениях, оборудованных датчиками пожарной сигнализации;

2) съем информации с датчиков различных типов (контактных, инфракрасных, радиотехнических и т.д.) (число датчиков, обслуживаемых системой, может составлять в зависимости от характера охраняемого объекта от 1 до 4 тысяч);

3) автоматическую постановку и снятие с охраны отдельных, зон (ворот, комнат, коридоров, гаражей и т.д.) с центрального пульта;

4) автоматическую постановку и снятие с охраны, отдельных помещений по индивидуальным кодам пользователей с использованием индивидуальных карточек) с регистрацией кода, Ф. И. О. владельца карточки, времени и места;

5) автоматическую подачу команд на внешние исполнительные устройства (разблокировку замков, включение видеокамер, сирен и т. п.);

6) организацию системы доступа в закрытые помещения (разблокировку замков) по индивидуальным карточкам владельцев;

7) экстренный вызов службы охраны в помещения объекта;

8) автоматический вывод информации на дисплей оператора, в тон числе графического плана охраняемого объекта с указанием расположения датчиков, установленных и снятых с охраны, места проникновения (или попытки), выхода из строя отдельных узлов системы и т. п;

9) запись, хранение, просмотр и распечатку всей информации (время постановки той или иной зоны под охрану, время и место нарушения, время

и место выхода из рабочего состояния датчиков, информация о работе оператора и т. д.);

10) автоматический непрерывный контроль за рабочим состоянием датчиков и узлов системы, автоматическое обнаружение попыток их несанкционированного вскрытия, повреждений линий связи;

11) автономное питание всех, периферийных узлов системы, в том числе энергопотребляющих датчиков.

Благодаря своей модульной структуре и гибкости программного обеспечения система может быть использована для охраны широкого класса

объектов, различающихся по расположению и числу охраняемых зон, числу и типу используемых датчиков, необходимому набору сервисных функций,

может совмещать функции охранной и противопожарной сигнализации.

В базовый состав системы входят:

1) центральный пульт управления (ЦПУ) на базе ПЭВМ IBM PC с принтером -1 шт.;

2) блок питания и обработки сигналов (БПОС) -1 шт.;

3) блок уплотнения (БУ) сигналов датчиков - от 1 до 256;

4) устройства вводя куда (УВК) с индивидуальных карточек - от 1

до512шт.; 5) средства обнаружения (контактные и бесконтактные датчики) - от 16

до 4096шт.;

6) четырехпроходные линии сбора/передачи информации и элек-

тропитания - от 1 до 8.

При необходимости система может дополняться ретрансляторами, позволяющими увеличить протяженность пиний связи.

Система отвечает требованиям стандартов Международной электротехнической комиссии и соответствующих отечественных ГОСТов.

Питание системы осуществляется от 1Люмьппленной сети переменного тока напряжением 220 В (+10; -15 %) частотой 50 Гц

(допускается питание от сети с частотой 60 Гц). Предусмотрено применение агрегата бесперебойного питания (АБП), обеспечивающего автоматическое переключение на резервное питание при пропадании основного и обратно.

Диапазон рабочих температур узлов системы:

а) ЦПУ, БПОС: 4-1... +40° С;

б) БУ, УВК: 40...+40° С.

Специализированное программное обеспечение позволяет формировать базы данных о конфигурации охраняемого объекта,

расположении датчиков и охранных зон, списке пользователей системы - владельцев индивидуальных карточек, с их индивидуальными кодами и

полномочиями по установке и снятию с охраны тех или иных зон или по проходу в те или иные закрытые помещения.

При необходимости система может быть дополнена аппаратными и программными средствами, позволяющими;

1) графически отображать план объекта с поэтажной разбивкой и указанием установленных под охрану и снятых, с охраны помещений, а также сработавших датчиков и охраняемых зон;

2) анализировать базы данных пользователей;

3) обрабатывать информацию из протокола системы.

Программное обеспечение позволяет формировать или корректировать конфигурацию объекта, базы данных, графический план без привлечения специалистов предприятия-изготовителя.

Приведем также общие сведения о сертифицированных технических средствах защиты.

По состоянию на январь 1996 г. сертификаты Государственный технической комиссии при Президенте РФ имеют следующие средства:

1) устройство защиты информаций от перехвата за счет излучений, возникающих при се выводе на дисплей ПЭВМ IBM PC (шифр «Салют»), разработанное научно-производственным государственным предприятием «Гамма» и фирмой «Криптон»; 2) техническая доработка ПЭВМ в целях снижения уровня побочных

электромагнитных излучений и наводок (ПЭМИН), произведенная научно-производственным концерном «Научный центр»;

3) техническая доработка персональных ЭВМ IBM PC-1 в целях снижения уровня ПЭМИН, произведенная акционерным обществом

«Российское научное товарищество»

4) средство активной защиты - генератор шума с диапазоном частот от 0,1 до 1000 МГц (шифр «ТШ-1000»), разработанное ЦНИИ машиностроения Российской коммерческой ассоциации;

5)такое же средство (шифр ГШ-К-1000), разработанное специальным конструкторским бюро Института радиоэлектроники Российской Академии наук;

6) защитное устройство подавления опасных сигналов в однофазных и трехфазных сетях электропитания (шифр «ФСКП-200(100)», разработанное научно-производственным предприятием «Элком»;

7) устройство запреты от прослушиваний помещения через телефонный аппарат, находящийся в режиме вызова (шифр «УЗТ»),

разработанное товариществом с ограниченной ответственностью «Предприятие ЛиК»; 8) такое же устройство (РАО019301) (шифр «Корунд»), разработанное

товариществом с ограниченной ответственностью «РЕНОМ»; 9)телевизионная система наблюдения (шифр «Виконт»), разработанная

научно-производственным объединением «Альфа-Прибор»

10) устройство защиты ПЭВМ от перехвата ПЭМИН объектов вычислительной техники 2 и 3 категорий в диапазоне частот Ш1000 МГц

(ИТСВ, 469435.006-02 ТУ), (шифр «Салют»), разработанное фирмой «Криптон».

В последнее время в особо важных АСОД (например, банковских)

стали применяться системы электронных платежей на основе пластиковых идентификационных карточек (ИК), которые известны также под названиями кредитные карточки, смарт-карты или «пластиковые деньги» и т. п. Название ИК более всего соответствует международным стандартам и основной их функции. ИК предназначены для осуществления взаимодействия человека с АСОД, поэтому могут быть определены как аппаратное средство АСОД в виде прямоугольной пластиковой карточки, предназначенное для

идентификации субъекта системы и являющееся носителем идентифицирующей информации.

Лабораторная идентификация пользователей заключается в установлении и закреплении за каждым пользователем АСОД уникального

идентификатора (признака) в виде номера, шифра, кода и т. д. Это связано с тем, что традиционный идентификатор вида ФАМИЛИЯ-ИМЯ-ОТЧЕСТЮ не всегда приемлем, уже хотя бы в силу возможных повторений и общеизвестности. Поэтому в различных автоматизированных системах широко применяется персональный идентификационный номер (ПИН).

ПИН обычно состоит та 4-12 цифр и вводится идентифицируемым пользователем с клавиатуры. На практике встречаются назначаемые или выбираемые ПИН. Последний устанавливается пользователем самостоятельно. Назначаемый ПИН устанавливается уполномоченным органом АСОД.

На практике существуют два основных способа проверки ПИН: алгоритмический и неалгоритмический. Алгоритмический способ проверки заключается в том, что у пользователя запрашивается ПИН, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением ПИН, хранящимся на карточке с соблюдением необходимых мер защиты. Главным достоинством этого метода проверки является отсутствие необходимости интерактивного обмена информацией в системе. При неалгоритмическом способе проверка ПИН осуществляется путем прямого сравнения ПИН на карте со значением,

хранимым в базе данных. Это обязывает использовать средства связи, работающие в реальном масштабе времени, и предусматривать средства зашиты информация в базе данных и линиях телекоммуникаций.

Идентификатор, используется при построении различных подсистем раз-граничения доступа.

Любая ИК используется в качестве носителя информации, необходимой для идентификации, и информации, используемой в других целях. Эта информация представляется и различных формах: графической,

символьной, алфавитно-цифровой, кодированной, двоичной. Множество форм представления информации на ИК объясняется тем, что карточка служит своеобразным связующим звеном между человеком (пользователем)

и машинной системой, для которых характерны различные формы представления информации.

Например, на карточку графически наносят специальный логотип, рисунок, фотографию, фамилию владельца, серийный номер, срок годности, штрих-код и т.п.

Логотип - графический символ организации, выпускающей карточку.

Он служит своеобразный знаком обслуживания, т.е. обозначением, дающим возможность отличать услуги одной организации от однородных услуг другой организации. Очевидно, что логотип должен обладать различительной способностью и не повторять общеупотребительные обозначения (гербы, флаги и т. п.). Для обеспечения безопасности изображение, в ток числе голографическое или видимое только в инфракрасных лучах, наносят на специальном оборудовании, что существенно затрудняет подделку карточки.

Другим средством повышения безопасности визуальной информации служит тиснение или выдавливание (эмбоссирование) некоторых идентификационных характеристик пользователя на поверхности ИК. Эти характеристики: с помощью специального устройства (импринтера) могут отпечатываться и дублироваться на бумажном носителе (слипе) доя дальнейшего учета.

В настоящее время нашли широкое применение магнитные, полу-проводниковые и оптические карточки, перечисленные в порядке снижения распространенности.

ИК нашли широкое применение в различных АСОД. Самое большое распространение карточек наблюдается в финансовой сфере.

Можно условно выделить три переплетающиеся области применения

И К.

1) электронные документы;

2) контрольно-регистрационные системы;

3) системы электронных платежей.

Карточки как средство контроля, разграничения и регистрации доступа к объектам, устройствам, информационным ресурсам АСОД используются при создании контрольно-регистрационных охранных систем. Например,

известны разнообразные электронные замки к помещениям и аппаратуре.

Разграничение доступа к данным ПЭВМ реализовано на уровне предъявления ключ-карты, содержащей идентификационные данные пользователя и его электронный ключ.

ИК являются ключевым элементом различных систем электронных платежей, в которых применяется около 1 миллиарда карточек.

Программные средства защиты

Программными средствами защиты информации называются специальные программы, которые включают в состав программного обеспечения АСОД для решения в них (самостоятельно или в комплексе с другими средствами) задач защиты. Программные средства являются важнейшей и непременной частью механизма защиты современных АСОД.

Такая роль определяется следующими их достоинствами: универсальностью» гибкостью, надежностью, простотой реализации, возможностью модификации и развития.

При этом под универсальностью понимается возможность решения программными средствами большого числа задач защиты.

Гибкость программных средств защиты заключается в двух характерных особенностях этого класса средств защиты: при параметрической реализации программ защиты они могут автоматически адаптироваться к конкретным условиям функционирования АСОД;

программные средства защиты могут быть адаптированы в структуре АСОД различным образом (могут быть включены в состав ОС и СУБД, могут

функционировать, как самостоятельные пакеты программ зашиты, их можно распределить между отдельными элементами АСОД и т. д.).

Под надежностью понимается высокая программная устойчивость при большой продолжительности непрерывной работы и удовлетворение

высоким требованиям к достоверности управляющих воздействий при наличии различных дестабилизирующих факторов.

Простота реализации программных средств защиты очевидна по сравнению с возможностью реализации любых других средств защиты.

Возможности изменения и развития программных средств защиты определяются самой их природой.

Основными недостатками использования программных средств защиты являются следующие: необходимость использования времени работы процессора, что ведет к увеличению времени отклика системы на запросы и,

как следствие, к уменьшению эффективности ее работы; уменьшение объемов оперативной памяти и памяти на внешних запоминающих устройствах, доступной для использования функциональными задачами;

возможности случайного или злоумышленного изменения, вследствие чего программы могут не только утратить способность выполнять функции защиты, но и стать дополнительным КИПИ; жесткая ориентация на архитектуру определенных типов ЭВМ (даже в рамках одного класса);

зависимость программ от особенностей базовой системы ввода-вывода, таблицы векторов прерываний и т. п.

Существенным недостатком программных средств зашиты является также возможность их реализации только в тех структурных элементах АСОД, где имеется процессор, хотя функции защиты могут реализовываться,

осуществляя безопасность других структурных элементов.

Аналогично техническим средствам в классификационной структуре программных средств определяющей является классификация по функциональному признаку, т, е. по классу задач зашиты, для решения которых предназначаются программы. Более того, исследований показывают,

что именно по этому критерию наиболее целесообразно выделять модули программных средств защиты, которые будут выступать элементарными типовыми проектными решениями (ТПР) программных средств. Поэтому идентификацию ТПР по программным средствам удобно осуществлять

цифровым кодом, состоящим из цифр, обозначающих вид задач защиты, номер класса задач, номер группы задач в классе, порядковый номер программы, предназначенной для решения задач данной группы.

Конкретный перечень программных средств защиты может быть самым различным; общее представление об их составе и содержании можно получить по следующему списку:

1) проверка прав доступа: по простому паролю, по сложному паролю, по разовым паролям;

2) опознавание пользователей по различным идентификаторам;

3) опознавание компонентов программного обеспечения;

4) опознавание элементов баз данных;

5) разграничение доступа к защищаемым данным по матрице полномочий, уровню секретности и другим признакам;

6) управление доступом к задачам, программам и элементам баз данных по специальным мандатам;

7) регистрация обращений к системе, задачам, программам и элементам защищаемых данных;

8) подготовка к выдаче конфиденциальных документов: формирование и нумерация страниц, определение а присвоение грифа конфиденциальности, регистрация выданных документов;

9) проверка адресата перед выдачей защищаемых данных в каналы связи;

10) управление выдачей данных в каналы связи;

11) криптографическое преобразование данных;

12) контроль процессов обработки и выдачи защищаемых данных;

13) уничтожение остаточной информации в ОЗУ после выполнения допросов пользователей;

14) сигнализация при попытках несанкционированных действий;

15) блокировка работы пользователей, нарушающих правила защиты информации;

16) организация псевдоработы с нарушителем в целях отвлечения его внимания;

17) программное обеспечение комплексных средств и систем защиты.

Для организационного построения программных средств до настоящего времени наиболее характерной является тенденция разработки комплексных программ, выполняющих целый ряд защитных функций,

причем чаще всего в число этих функций входит опознавание пользователей,

разграничение доступа к массивам данных, запрещение доступа к некоторым областям ЗУ и т. п.

Достоинства таких программ очевидны: каждая из них обеспечивает решение некоторого числа важных задач защиты. Но им присущи и существенные недостатки, предопределяющие необходимость критической оценки сложившейся практики разработки и использования программных средств защиты. Первый и главный недостаток состоит в стихийности развития программ защиты, что, с одной стороны, не дает гарантий полноты имеющихся средств, а с другой - не исключает дублирования одних и тех. же задач защиты. Вторым существенным недостатком является жесткая фиксация в каждом из комплексов программ защитных функций, И еще один большой недостаток - ориентация подавляющего большинства имеющихся программных средств на конкретную среду применения: тип ЭВМ и операционную систему.

Отсюда вытекают три принципиально важных требования к формированию программных средств: функциональная полнота, гибкость и унифицированность использования.

Что касается первого требования, то, как нетрудно убедиться, приведенный выше перечень программных средств составлен именно с таким расчетом, чтобы возможно более полно охватить все классы задач защиты.

Удовлетворение остальным двум требованиям зависит от форм и способов представления программ зашиты. Анализ показал, что наиболее

полно требованиям гибкости и унифицированности удовлетворяет следующая совокупность принципов: сквозное модульное построение,

полная структуризации, представление на машинонезависимом языке.

Принцип сквозного модульного построения заключается в том, что каждая из программ любого уровня (объема) должна представляться в виде системы вложенных модулей, причем каждый такой модуль должны быть полностью автономным и иметь стандартные вход и выход обеспечивающие комплексирование с любыми другими модулями. Нетрудно видеть, что эти условия могут быть обеспечены, если программные комплексы будут разрабатываться по способу сверху-вниз.

Представление на машинонезависимом языке предопределяет, что представление программных модулей должно быть таким, чтобы их с минимальными усилиями можно было включить в состав программного обеспечения любой АСОД. Как известно, в настоящее время имеются алгоритмические языки высокого уровня, трансляторы с которых включены в состав программного обеспечения наиболее распространенных ЭВМ.

Такими, например, являются Паскаль, Ада и др. Однако универсализацию представления программных модулей можно расширить еще больше, если каждый их этих модулей представить в виде блок-схемы, детализированной до такой степени, что каждый из блоков может быть реализован одним -

двумя операторами наиболее распространенных языков высокого уровня или ограниченным числом команд на языке Ассемблера. Тогда конкретная реализация программы будет заключаться в простом кодировании блоков соответствующих блок-схем.

По состоянию на январь 1996 г. сертифицированы следующие программные средства защиты:

1) система защиты информации от НСД для ПЭВМ (по 4-му классу защищенности) (шифр «Кобра»), разработанная ГНИИ моделирования и

интеллектуальных сложных систем и акционерным обществом закрытого типа «Кобра-ЛАЙН»;

2) программный комплекс защиты информации от НСД дня ПЭВМ (по

2-му классу защищенности) (шифр «Страж 1.1»), разработанный войсковой часть 01168;

3) комплекс программных средств защиты от НСД для персонального компьютера «МАРС» (КПСЗИ «МАРС») - по 3-му классу защищенности,

разработанный Российским центром «Безопасность»; 4) система защиты информации от НСД в ЛВС - по классу

защищенности 1Д (ЛВС) и 6 классу защищенности для СВТ (шифр «Сизам»),

разработанная научно-производственной фирмой «Кристалл».

В последние годы сформировалась довольно устойчивая тенденция создания комплексных программно-технических и программно-аппаратных средств защиты, предназначенных для решения некоторого набора взаимосвязанных задач защиты. В подтверждение сказанному ниже приводится перечень сертифицированных комплексных средств:

1) система защиты информации от НСД для ПЭВМ IBM PC XT/AT (шифр «Снег 2.0»), разработанная ЦНИИАтоминформом Минатома России;

2) система защиты информации от НСД в ЛВС (шифр «Снег-ЛВС»),

разработанная названной выше организацией;

3) закрытая часть электронного почтамта центрального узла сети

(шифр «УралВЭС»), разработанная товариществом с ограниченной ответственностью «Микротест»;

4) встроенная система парольной защиты загрузки ПЭВМ РСД-4 Gsx/25 фирмы Siemens Nizdorf, разработанная управлением информационных ресурсов Администрации Президента;

5) электронный ключ на базе программируемого постоянного запоминающего устройства (по 6 классу защищенности) (шифр «Dallas Lock»), разработанный акционерным обществом «Конфидент»;

6) программно-техническая доработка изделия 83т 744 от НСД к информации, выполненная НИИ автоматической аппаратуры;

7) автоматизированный кассовый аппарат на базе ЭВМ IBM PC с системой защиты и разграничением доступа (шифр IPC ЮЗ IIS#P), разработанный фирмой «ПИЛОТ»;

8) единичный образец программно-аппаратного комплекса «Аккорд» (СТЮИ.00506-01 ТУ защиты ПЭВМ от НСД (шифр «Аккорд»), разработанный ОКБ САПР;

9) автоматизированная система безналичных расчетов «БЛИЦ», функционирующая совместно с СЗИ от НСД QP DOS ТК (шифр АСБН «БЛИЦ»), разработанная акционерным обществом закрытого типа «БЛИЦ-ЦЕНТР»; 10) автоматизированный программно-аппаратный комплекс по

управлению и расчету автозаправочных предприятий (шифр «Кютан-С» разработанный акционерный обществом «Центр технического обслуживания ККМ»;

11) програмно-аппаратный комплекс защиты от НСД и обработки конфиденциальной информации DALLAS Lock 34, разработанный Ассоциацией защиты информации «Конфидент»;

12) система, защиты локальной вычислительной сети «SECRET NET», верам 1.10 (включая ее локальную версию) - до 6 классу защищенности для СВТ, разработанная акционерным обществом закрытого типа «Информзащита».

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Изучить классификацию технических средств защиты

3. Ознакомиться с описанием способов защиты пластиковых идентификационных карт

4. Изучить перечень программных средств защиты, требования к формированию программных средств

5. Оформить отчет

Содержание отчета и его форма

Отчет должен иметь форму согласно оформлению простого реферата.

Титульный лист должен включать название дисциплины, название практической работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической работы должна содержать:

1. Классификацию технических средств защиты

2. Классификацию технических средств защиты по функциональному назначению

3. Описание способов защиты пластиковых идентификационных карт

4. Перечень программных средств защиты, требования к формированию программных средств

5. Выводы по проделанной работе

Вопросы для защиты работы

1. Дайте определение, приведите и обоснуйте классификацию технических средств защиты информации
2. Раскройте назначение, принципы действия и приведите примеры технических средств внешней защиты
3. Раскройте назначение, принципы действия и приведите примеры технических средств опознавания
4. Раскройте назначение, принципы действия и приведите примеры технических средств внутренней защиты

5. Дайте определение, приведите и обоснуйте классификацию программных средств защиты информации

Лабораторная работа № 8

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ОРГАНИЗАЦИОННЫХ СРЕДСТВ ЗАЩИТЫ

Цель и содержание: провести исследование особенностей организационных средств защиты

Теоретическое обоснование

В соответствии с определением, организационными средствами защиты названы организационно-технические и организационно-правовые мероприятия, осуществляемые: в процессе проектирования, создания и эксплуатации АСОД с целью защиты информации. Организационные средства играют особую роль в общем механизме защиты, что обусловлено повышенным влиянием случайных факторов на защищенность информации,

а важнейшей отличительной чертой рассматриваемых средств является их способность учитывать случайные факторы (неформальный характер).

Следующее важное обстоятельство, которое непременно должно учитываться при разработке организационных средств, заключается в особой, тройственной их роли в механизмах защиты информации; они, во-

первых позволяют непосредственно решать (самостоятельно или в комплексе с другими средствами) задачи защиты, во-вторых, обеспечивают эффективное использование средств других классов, а, в-третьих, позволяют рациональным образом объединить вес средства в единую, целостную систему защиты. Сказанное предопределяет необходимость более пристального внимания к организационным средствам, отличительными особенностями которых являются:

1) всеобщность, т, е. актуальность использования их для решения широкого круга задач защиты во всея компонентах АСОД, на всех этапах их

жизненного цикла и во всех ситуациях, которые имеют или могут иметь место в процессе автоматизированной обработки информации;

2) явно выраженная ненормальность, т. е. возможность разработки и реализации их только при непременном и активном участии людей;

3) специфичность, т.е. возможность эффективной разработки и реализации при условии высокой профессиональной подготовки специа-

листов, участвующих в разработке и реализации; 4) высокий уровень неопределенности, т. е. невозможность фор-

мального определения точных границ и эффективности их действия.

Перечисленными особенностями обусловливаются два существенных обстоятельства: 1) множество все необходимых и потенциально возможных организационных средств является неопределенным; 2) не существует формальных методов формирования перечня и содержания организационных средств.

Исходя их этого, основными методами формирования организаци-

онных средств: могут быть только неформально-эвристические методы в различных модификациях. Рассматриваемые ниже средства формировались именно такими методами. Для этого была разработана приводимая ниже классификационная структура организационных средств, затем методами экспертных суждений формировались перечни средств каждой группы.

Дополнительным пособием в этой работе послужили имеющиеся публикации по различным аспектам защиты информации.

Отличительные особенности организационных средств обусловливают и особенности их использования, самой важной из которых является та, что защитные функции организационных средств могут быть реализованы лишь как результат целенаправленной деятельности людей, имеющих отношение к автоматизированной обработке защищаемой информации. Отсюда вытекает ряд следствий, основными из которых следует назвать следующие: люда,

реализующие организационные средства, должны: иметь стимулы, побуждающие: их эффективно реализовывать все организационные средства, они должны быть подготовлены к реализации этих средств, и они должны быть обеспечены всем необходимым для их реализации.

На основе анализа сущности и места организационных средств в общей структуре, средств СЗИ нетрудно заключить, что для системной классификации рассматриваемых средств представительной будет сле-

дующая совокупность критериев: этапы жизненного цикла системы защиты информации, функции организационных средств, сфера действия организационных средств.

В таблице 3 приведены общие данные, характеризующие структуру перечисленных критериев.

Таблица 3 – Структуризация критериев системной классификации организационных средств защиты информации

№№ п/п	Наименование	Общая характеристика критерия	Значение критерия	Характеристика значения критерия
1	Функции организационных средств	Характеризует назначение организационных средств них место в общей совокупности средств защиты	Непосредственная защита информации Поддержка других средств Объединение средств защиты в единую систему	Выделяет те организационные средства, применением которых (самостоятельно или в совокупности с другими) обеспечивается полное или частичное перекрытие одного или нескольких каналов несанкционированного получения информации Выделяет те организационные средства, которые необходимы (целесообразны) для эффективного функционирования других средств Выделяет те организационные средства, которые необходимы (целесообразны) для эффективного объединения всех используемых средств в единую систему защиты информации
2	Этапы жизненного цикла системы за-	Характеризует тот интервал времени в течение	Проектирование	Выделяет те организационные средства, которые необходимы (целесообразны) на этапе проектирования СЗИ

	щиты информации	которого используются	Внедрение	Выделяет те организационные средства, которые необходимы

		органи-зационные средства			(целесообразны) на этапе внедрения СЗИ
				Эксплуатация	Выделяет тс организационные средства, которые необходимы (целесообразны) на этапе эксплуатации СЗИ
3	Сфера действия средств	Характеризует те субъекты, объекты или процессы, на которые распространяется действие организационных средств		Общего назначения	Выделяет те организационные средства, которые носят всеобщий характер
				Направленные на структурные компоненты АСОД	Выделяет те организационные средства, которые регламентируют построение иди функционирование технического, математического, программного, информационного или лингвистического обеспечения АСОД
				Направленные на технологию автоматизированной обработки информации	Выделяет те организационные средства, которые регламентируют построение или функционирование технологии автоматизированной обработки защищаемой информации
				Направленные на людей	Выделяет те организационные средства, которые регламентируют деятельность людей, участвующих в автоматизированной обработке информации

Тогда классификационная структура организационных средств будет выглядеть так, как показано на рисунке 5.

Рисунок 5 – Классификационная структура организационных средств защиты информации

Полное множество элементов классификационной структуры организационных средств определяется декартовым произведен нем значений всех составляющих критериев системной классификации. Каждый элемент образованного таким образом множества представляет собой группу однородных организационных средств. Конкретный же перечень средств может быть самым различным. Целенаправленно проводимые организационно-технические и организационно-правовые мероприятия непременно должны сопровождать все процессы, каким-либо образом имеющие отношение к обработке защищаемой информации.

Ниже для иллюстрации приводится перечень некоторых организационных, мер защиты:

1) организация разработки, внедрения и использования средств и систем защиты;

2) управление доступом персонала на территорию, в здания и помещения объекта путем проверки пропусков;

3) контроль состояния и использования технических средств, документов, машинных носителей информации и других компонентов АСОД;

4) контроль соблюдения правил защиты информации пользователями и персоналом АСОД;

5) планирование и организация обработки защищаемой информации;

6) подбор, расстановка и подготовка кадров, участвующих в обработке защищаемой информации:

7) организация уничтожения бумажных документов, содержащих защищаемую информацию, надобность в которых, миновала;

8) организация ведения архивных массивов данных и документов;

9) ведение журналов регистрации сбоев и отказов средств и систем защиты;

10) организация учета и обработки сведений об обнаруженных удачных и неудачных попытках несанкционированных действий в АСОД;

11) организация и проведение профилактических осмотров и ремонта средств и систем защиты информации;

12) анализ функционирования средств и систем защиты информации в целях их совершенствования;

13) разработка и внедрение в практику инструкций и других документов, регламентирующих правила обращения с защищаемой информацией.

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Изучить классификационную структуру организационных средств защиты информации

3. Рассмотреть перечень организационных мер защиты

4. Оформить отчет

Содержание отчета и его форма

Отчет должен иметь форму согласно оформлению простого реферата.

Титульный лист должен включать название дисциплины, название практической работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической работы должна содержать:

1. Структуризацию критериев системной классификации организационных средств защиты информации

2. Классификационную структуру организационных средств защиты информации

3. Перечень организационных мер защиты

4. Выводы по проделанной работе

Вопросы для защиты работы

1. Дайте определение, приведите и обоснуйте классификацию организационно-правовых средств защиты

2. Раскройте назначение, приведите перечень и краткое содержание организационных мероприятий общего характера

3. Раскройте назначение, приведите перечень и краткое содержание мероприятий, осуществляемых на разных этапах функционирования систем защиты.

Лабораторная работа № 9

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

Цель и содержание: провести исследование особенностей криптографических средств защиты

Теоретическое обоснование

Криптографическое закрытие является специфическим способом защиты информации, оно имеет многовековую историю развития и применения. Поэтому у специалистов не возникало сомнений в том, что эти средства могут эффективно использоваться также и для защиты информации

В АСОД, вследствие чего им уделялось и продолжает уделяться большое внимание. Достаточно сказать, что в США еще в 1978 г. утвержден а рекомендован дня широкого применения национальный стандарт криптографического закрытия информации. Подобный стандарт в 1989 г,

утвержден и у нас в стране. Интенсивно ведутся исследования с целью разработки высоко стойких и гибких методов криптографического закрытия информации. Более того, сформировалось самостоятельное научное направление - криптология, изучающая и разрабатывающая научно-

методологические основы, способы, методы и средства криптографического преобразования информации.

Можно выделить следующие три периода развития криптологии,

Первый период - эра донаучной криптологии, являвшейся ремеслом-уделом узкого круга искусных умельцев. Началом второго периода можно считать

1949 год, когда появилась работа К. Шеннона «Теория связи в секретных системах», в которой проведено фундаментальное научное исследование

шифров и важнейших вопросов их стойкости. Благодаря этому труду криптология оформилась как прикладная математическая дисциплина. И,

наконец, начало третьему периоду было положено появлением в 1976 г.

работы У. Диффи, М. Хеллмана «Новые направления в криптографии», где показано, что секретная связь возможна без предварительной передачи секретного ключа. Так началось и продолжается до настоящего времени бурное развитие наряду с обычной классической криптографией и криптографии с открытым ключом.

Приведем краткую историческую справку развития криптографии.

Еще несколько веков назад само применение письменности можно было рассматривать как способ закрытия информации, так как владение письменностью было уделом немногих.

XX в. до н. э. При раскопках в Месопотамии был найден один из самых древних шифртекстов. Он был написан клинописью на глиняной табличке и содержал рецепт глазури для покрытия гончарных изделий что, по-

видимому, было коммерческой тайной. Известны древнеегипетские религиозные тексты и медицинские рецепты.

Середина IX в. до н. э. Именно в это время, как сообщает Плутарх использовалось шифрующее устройство - скиталь, которое реализовывало по так называемый шифр перестановки. При шифровании слова писались на узкую ленту, намотанную на цилиндр, вдоль образующей этого цилиндра

(скиталя). После этого лента разматывалась и на ней оставались переставленные буквы открытого текста. Неизвестным параметром ключом -

в данном случае служил диаметр этого цилиндра. Известен и метод дешифрования такого шифр текста, предложенный Аристотелем, который наматывал ленту на конус, и то место, где появлялось читаемое слово или его часть, определяло неизвестный диаметр цилиндра.

56 г. н. э. Во время войны с галлами Ю. Цезарь использует другую разновидность шифра - шифр замены. Под алфавитом открытого текста писался тот же алфавит со сдвигом (у Цезаря на три позиции) по циклу. При шифровании буквы открытого текста у верхнего алфавита заменялись на буквы нижнего алфавита. Хотя этот шифр был известен до Ю. Цезаря, тем не менее шифр был назван его именем. Другим более сложным шифром замены является греческий шифр – «квадрат Полибия». Алфавит записывается в виде квадратной таблицы. При шифровании буквы открытого текста заменялись на пару чисел - номера столбца и строки этой буквы в таблице. При произвольном расписывании алфавита по таблице и шифровании такой таблицей короткого сообщения,

этот шифр является стойким даже по современным понятиям. Идея была реализована в более сложных шифрах, применявшихся во время первой мировой войны.

Крах Римской империи в V в н. э. сопровождался закатом искусства и наук, в том числе и криптографии. Церковь в те времена преследовала тайнопись, которую она считала чернокнижием и колдовством. Сокрытие мыслей за цифрами не позволяло церкви контролировать эти мысли.

Р. Бэкон (1214-1294) - францисканский монах и философ - описал семь систем секретного письма. Большинство шифров в те времена применялись для закрытия научных записей.

Вторая половина XV в. Леон Баттиста Альберти, архитектор и математик, работал в Ватикане, автор книги о шифрах, где описал шифр замены, на основе двух концентрических кругов, по периферии которых были нанесены на одном круге - алфавит открытого текста, а на другом -

алфавит шифр текста. Важно, что шифр алфавит был не последовательным и мог быть смещен на любое количество шагов. Именно Альберти впервые применял для дешифрования свойство неравномерности встречаемости

различных букв в языке. Он впервые также предложил для повышения стойкости применять повторное шифрование с помощью разных шифр систем.

Известен факт, когда король Франции Франциск I в 1546 году издал указ, запрещающий подданным использование шифров. Хотя шифры того времени были исключительно простыми, они считались нераскрываемыми.

Иоганн Тритемий (1462-1516) - монах-бенедиктинец, живший в Германии, Написан один из первых учебников по криптографии. Предложил

оригинальный шифр многозначной замены под названием «Ave Maria».

Каждая буква открытого текста имела не одну замену, а несколько, по выбору шифровальщика. Причем буквы заменялись буквами или словами так, что получался некоторый псевдооткрытый текст, тем самым скрывался сам факт передачи секретного сообщения. То есть применялась стеганография вместе с криптографической защитой. Разновидность шифра многозначной замены применяется до сих пор. Например, в архиваторе ARJ.

Джироламо Кардано - итальянский математик, механик, врач, изобрел систему шифрования, так называемую решетку Кардано, на основе которой,

например, был создан один из наиболее стойких военно-морских шифров Великобритании во время второй мировой войны. В куске картона с размеченной решеткой определенным образом прорезались отверстия,

нумерованные в произвольном порядке. Чтобы получил шифр текст, нужно положить этот кусок картона на бумагу и начинать вписывать в отверстия буквы в выбранном порядке. После снятия картона промежутки бессмысленного набора букв дописывались до псевдосмысловых фраз, так можно было скрыть факт передачи секретного сообщения. Скрытие легко достигается, если промежутки эти большие и если слова языка имеют небольшую длину, как, например, в английском языке. «Решетка Кардано» -

это пример шифра перестановки.

XVI в. Шифры замены получили развитие в работах итальянца Джованни Батиста Порты (математик) и француза Блеза де Вижинера

(дипломат).

Система Вижинера в том или ином виде используется до настоящего времени, поэтому ниже она будет рассмотрена достаточно детально.

XVII в. Кардинал Ришелье (министр при короле Франции Людовике XШ) создал первую в мире шифр службу.

Лорд Френсис Бэкон (1562-1626) был первым, кто обозначил буквы 5-значным двоичным кодом: A = 00001, B = 00010,… и т. д. Правда, Бэкон никак не обрабатывал этот код, поэтому такое закрытие было совсем

нестойким. Просто интересно, что через три века этот принцип был положен в основу электрической и электронной связи. Тут уместно вспомнить коды Морзе, Бодо, международный телеграфный код № *2*, код ASCII, также представляющие собой простую замену.

В этом же веке были изобретены так называемые словарные шифры. При шифровании буквы открытого текста обозначались двумя числами -

номером строки и номером буквы в строке на определенной странице какой-

нибудь выбранной распространенной книги. Эта система является довольно стойкой, но неудобной. К тому же книга может попасть в руки противника.

В конце XVIII века в переписке французской метрополии с колониями стали широко применяться коды, в основном трехзначные, на несколько сот кодвеличин. Обычно при кодировании пользуются кодкнигой, где для удобства все кодвеличины стоят в алфавитном порядке. Если при кодировании нужного слова не окажется среди кодвеличин, то оно кодируется побуквенно. Код имеет только один ключ - долговременный содержание кодкниги.

К.Гаусс (1777-1855) - великий математик тоже не обошел своим вниманием криптологию. Он создал шифр, который ошибочно считал нераскрываемым. При его создании использовался интересный прием -

рандомизация (random - случайный) открытого текста. Открытый текст можно преобразовать в другой текст, содержащий символы большего алфавита, путем замены часто встречающихся букв случайными символами из соответствующих определенных им групп. В подучающемся тексте все символы большого алфавита встречаются с примерно одинаковой частотой. Зашифрованный таким образом текст противостоит методам раскрытия на основе анализа частот появления отдельных символов. После расшифрования

законный получатель легко снимает рандомизацию. Такие шифры называют «шифрами с многократной подстановкой» или «равночастотными шифрами».

Ниже будет приведен пример такого шифра.

Перейдем теперь к рассмотрению криптографических средств применительно к потребностям защиты информации в современных АСОД.

Как известно, до недавнего времени криптографические средства использовались преимущественно (если не всецело) для сохранения государственной тайны, поэтому сами средства разрабатывались специальными органами, причем использовались криптосистемы очень высокой стойкости, что, естественно, сопряжено было с большими затратами. Однако, поскольку сфера защиты информации в настоящее время резко расширяется, становится весьма целесообразным системный анализ криптографических средств с учетом возможности и целесообразности их широкого применения для сохранения различных видов секретов и в различных условиях. Кроме того, в последние годы интенсивно разрабатываются новые способы криптографического преобразования данных, которые могут найти более широкое по сравнению с традиционными, применение.

В связи с изложенным, представляется целесообразным рассмотреть следующую совокупность вопросов:

1) возможности применения криптографических методов в АСОД;

2) основные требования к криптографическому закрытию информации в АСОД;

3) методы криптографического преобразования данных;

4) проблемы реализации методов криптографической защиты в АСОД;

5) характеристики криптографических средств защиты;

6) новые криптографические методы и их использование.

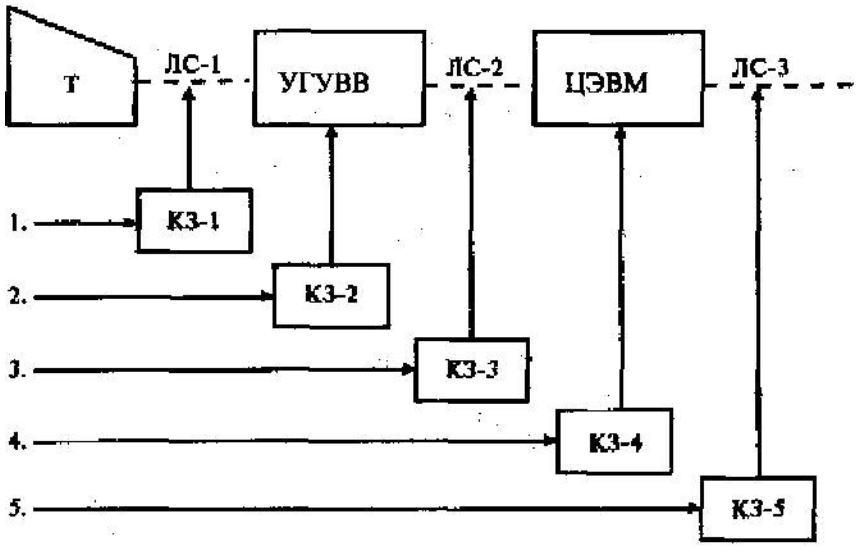


Рисунок 1 – Возможности использования криптографических методов

Возможность применения криптографических методов в АСОД.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Поэтому криптографические методы могут использоваться как внутри отдельных устройств или звеньев системы, так и на различных участках линий связи. Возможные узлы и точки автоматизированных систем, в которых могут применяться криптографические методы, показаны на рисунке 1.

В первом варианте (блок КЗ-1) обеспечивается закрытие информации, передаваемой между терминалом пользователя и устройством группового управления вводом-выводом данных (УГУВВ), вариант № 2 (блок КЗ-2)

предусматривает защиту информации, хранимой и обрабатываемой в УГУВВ, в варианте № 3 обеспечивается защита информации в линии связи между УГУВВ и ЦЭВМ (центральная ЭВМ сети). В варианте № 4 защищается информация, хранимая и перерабатываемая в ЦЭВМ, и, наконец, вариант № 5 означает защиту информации, передаваемой по линиям связи

между ЦЭВМ и внешними абонентами (например, другими автоматизированными системами, некоторыми исполнительными

устройствами и т. д.). Необходимость и целесообразность использования любого из названных вариантов защиты информации определяются степенью конфиденциальности обрабатываемой в каждом структурном элементе системы информации и конкретными условиями размещения и функционирования различных элементов автоматизированной системы.

Само собой разумеется, что возможно применение любых комбинаций названных вариантов защиты.

Основные требования к криптографическому закрытию информации в АСОД. К настоящему времени разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющее число этих методов может быть успешно использовано и для закрытия информации в АСОД. Наличие в составе таких систем быстродействующих процессоров и ЗУ большого объема значительно расширяет возможности криптографического закрытия. Так как криптографические методы при правильном применении обеспечивает высокую эффективность защиты, то они широко используются в системах различного типа.

Однако для того, чтобы криптографическое преобразование обеспечивало эффективную защиту информации в АСОД оно должно удовлетворять ряду требований. Эти требования были выработаны в процессе практического применения криптографии, часть их основана на технико-экономических соображениях. В сжатом виде их можно сформулировать следующим образом:

1) сложность и стойкость криптографического закрытия должны выбираться в зависимости от объема и степени секретности данных;

2) надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод закрытия;

3) метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными;

4) выполнение процедур прямого и обратного преобразований должно быть формальным. Эта процедуры не должны зависеть от длины сообщений;

5) ошибки, возникающие в процессе выполнения преобразования» не должны распространяться по системе;

6) вносимая процедурами защиты избыточность должна быть минимальной.

Методы криптографического преобразования данных. В настоящее время не существует общепринятой классификации криптографических методов. Но судя по большинству опубликованных работ, наиболее целе-

сообразной представляется классификация, показанная на рисунке 2.

Под шифрованием в данном случае понимается такой вид криптографического закрытия, при которой преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования можно разбить на пять групп: подстановка (замена),

перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование. Каждый из этих способов может иметь несколько разновидностей, некоторые из которых показаны на схеме.

Под кодированием понимается такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами

(цифровыми, буквенными, буквенно-цифровыми сочетаниями и т л.). Этот метод имеет две разновидности: смысловое и символьное кодирование. При смысловом кодировании кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложении). При символьном кодировании кодируется каждый символ защищаемого сообщения.

Символьное кодирование по существу совпадает с шифрованием заменой.

К отдельным видам криптографического закрытия отнесены методы рассечения-разнесения и сжатия данных. Рассечение-разнесение заключается

в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть

содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам ЗУ или располагаются на различных носителях. Сжатие данных представляет собой замену часто встречающихся одинаковых строк данных или последовательностей одинаковых символов некоторыми заранее выбранными символами.

Простые системы криптографического преобразования. Простыми названы такие системы, которые, с одной стороны весьма просты в реализации, а с другой - могут обеспечить достаточно надежную защиту, по крайней мере небольших объемов информации и на не очень большие интервалы времени. Из таких систем рассмотрим усложненные замены или подстановки (по так называемой таблице Вижинера и монофонической заменой), усложненные перестановки (с использованием так называемых пустышек и по маршрутам Гамильтона), гаммированием, аналитическим преобразованием, а также кодированием и рассечением-разнесением.

Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n - число символов используемого алфавита. На рисунке 3

показана таблица Вижинера для русского языка. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матриц па шифрования. Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею - строки,

соответствующие буквам ключа в порядке следования этих букв в ключе.

Пример такой рабочей матрицы для ключа САЛЬЕРИ приведен в средней части рисунке 4.

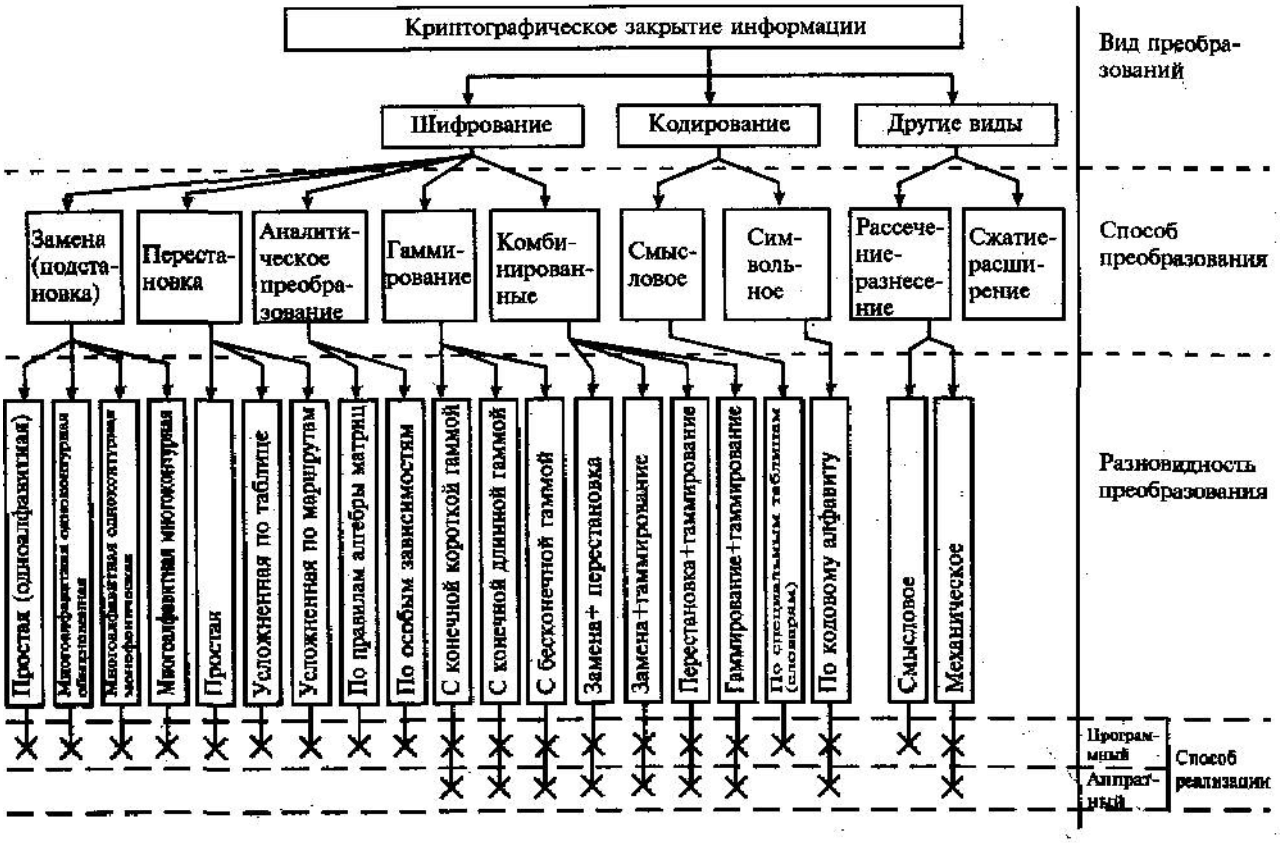


Рисунок 2 – Классификация криптографических методов преобразования информации

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я
б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а
в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б
г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в
д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г
е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д
ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е
з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж
и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з
й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и
к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й
л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к
м н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л
н о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м
о п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н
п р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о
р с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п
с т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р
т у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с
у ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т
ф х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у
х ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф
ц ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х
ч ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц
ш щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч
щ ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш
ь ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ
ъ ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь
ы э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ
э ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы
ю я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э
я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ь ъ ы э ю

Рисунок 3 – Таблица Вижинера дня русского алфавита

Рисунок 4 – Порядок шифрования по таблице Вижинера с использованием ключа «Сальери»:

ОТ - открытый текст, ШТ - шифрованный текст

Сам процесс шифрования осуществляется следующим образом: 1) под каждой буквой шифруемого теста записываются буквы ключа, и ключ при этом повторяется необходимое число раз; 2) каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и строк находящихся под ними букв ключа; 3) полученный текст может разбиваться на группы по несколько знаков.

Пусть, например, требуется зашифровать сообщение; МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ ПЯТЬСОТ РУБ. ЗА ШТУКУ. В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ
САЛЬЕРИСАЛЬ ЕРИСАЛЬЕРИ САЛЬЕ РИСАЛЬЕР
ПЯТЬСОТ РУБ. ЗА ШТУКУ ИСАЛЬЕР ИСА ЛЬ ЕРИСА Дальше осуществляется непосредственное шифрование в соответствии

со вторым правилом, а именно: берем первую букву шифруемою текста (М) и соответствующую ей букву ключа (С); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под нею букву, расположенную в строке соответствующей букве ключа (С) - в нашем примере такой буквой является Э; выбранную таким образом букву помещаем в шифрованный текст. Эта процедура циклически повторяется до зашифрования всего текста.

На рисунке 4 схема шифрования представлена в наглядном виде.

Исследования показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Нетрудно видеть, что замена по

таблице Вижинера эквивалентна простой замене с циклическим изменением алфавита, т. е. здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове-ключе. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т, е. на число букв в ключе.

Расшифрование текста производится в следующей последовательности:

1) над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое числа раз;

2) в строке подматрицы Вижннера, соответствующей букве ключа отыскивается буква, соответствующая знаку зашифрованного текста.

Находящаяся под ней буква первой строки подматрицы и будет буквой ис-

ходного текста; 3) полученный текст группируется в слова
по смыслу.

Нетрудно видеть, что процедуры как прямого, так и обратного преобразований являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по иному и тому же алгоритму. На рисунке 5 приведена укрупненная блок-схема такого алгоритма.

Одним из недостатков шифрования по таблице Вижинера является го,

что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает, В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющую смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведем некоторые из них: 1) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке; 2) в качестве ключа используются случайные

последовательности чисел. Из таблицы Вижинера выбираются десять Произвольных строк, которые кодируются натуральными числами от 0 до 10,

Эти строки используются в соответствии с чередованием цифр в выбранном ключе. В литературе приводятся и другие модификации метода.

Частным случаем рассмотренной поалфавитной замены является так называемая монофоническая замена. Особенность этого метода состоит в том, что количество и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки.

Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих элементов, чем для редко встречающихся. Пример монофонического шифра для английского алфавита показан на рисунке 6. Шифрование осуществляется так же, как и при простой замене с той лишь разницей, что после шифрования каждого знака соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию. Таким образом, столбцы алфавита как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака. В качестве примера зашифруем монофоническим шифром текст:

In this book the reader will

Шифрованный текст имеет вид:

A(--,) VNC/LjpGZ+f.] = hq^O…

Подсчитав частоты появления символов, мы увидим, что даже на таком коротком образце текста они в значительной мере выровнены. При увеличении объема текста частоты появления символов будут еще больше выравниваться.

Усложнение перестановки по таблице заключается в том, что для записи символов шифруемого текста используется специальная таблица, в

которую введены некоторые усложняющие элементы. Пример такой таблицы приведен на рисунке 12. Как следует из рисунка, таблица представляет собой матрицу размерами 10x10 элементов (размеры могут быть выбраны произвольно), в которую, записываются знаки шифруемого текста.

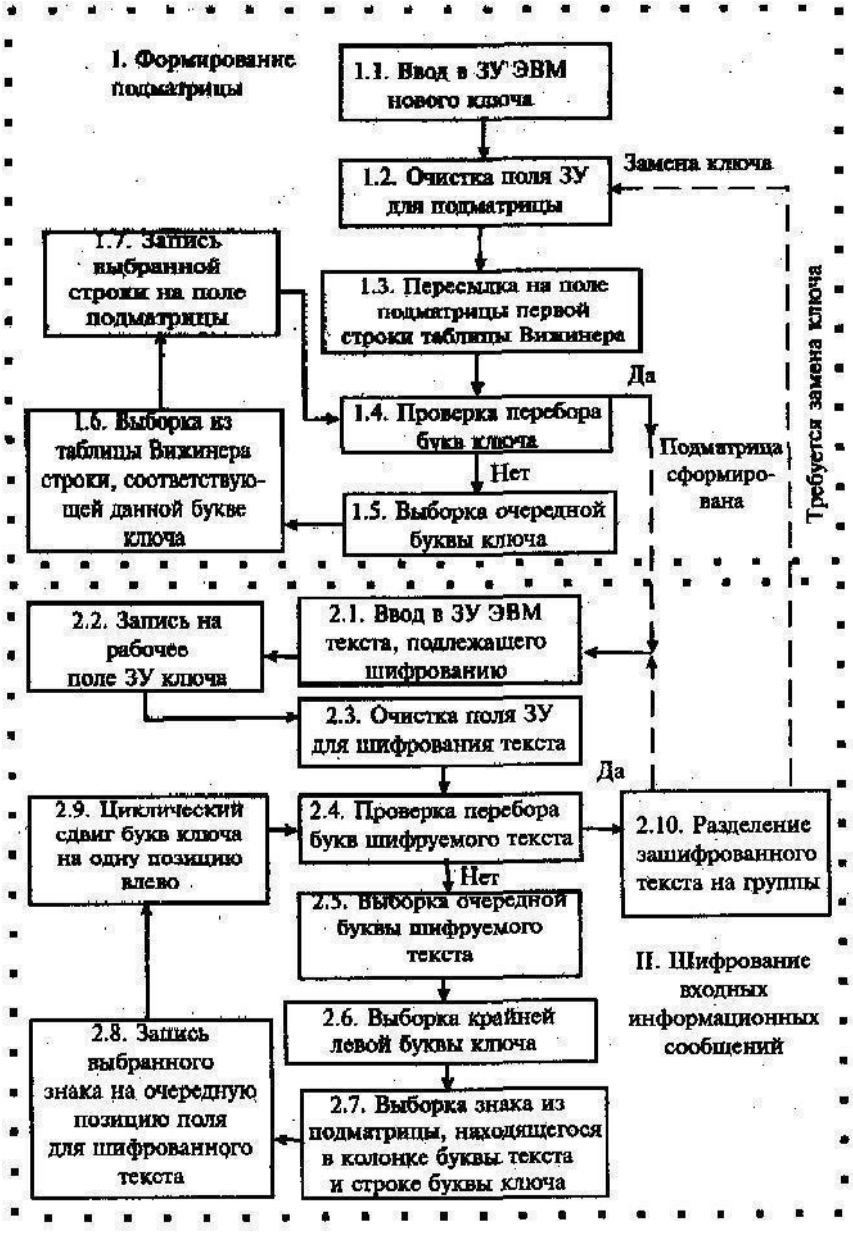


Рисунок 5 – Укрупненная схема алгоритма шифрования по таблице Вижинера

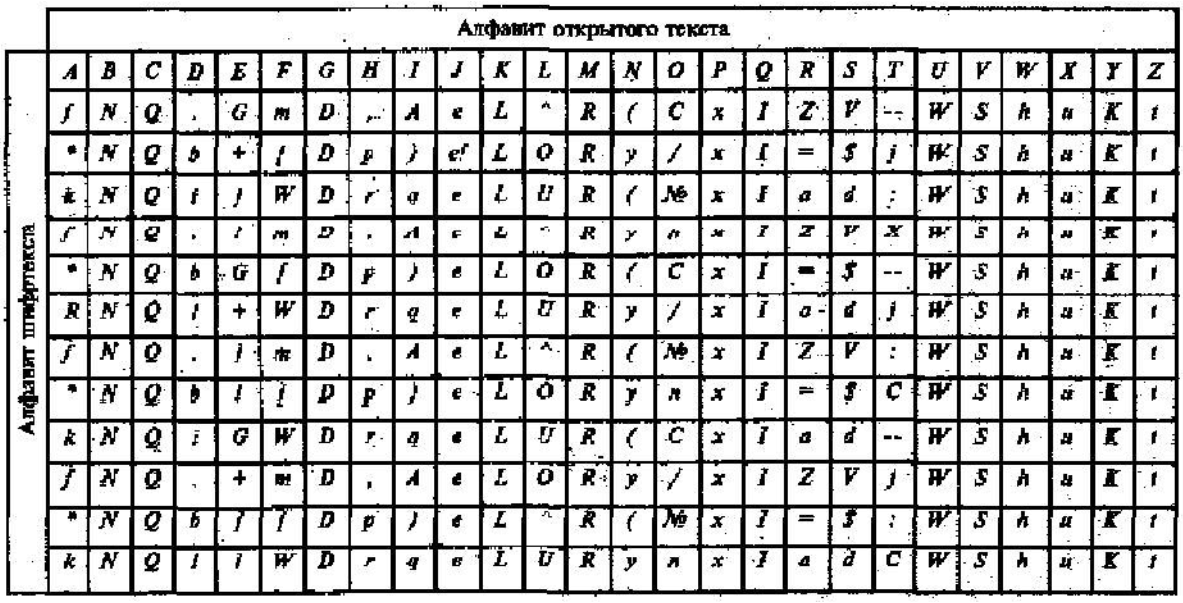


Рисунок 6 – Монофонический шифр для английского алфавита Усложнение состоит в том, что определенное число клеток таблицы не

используется (на рисунке они заштрихованы). Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования.

Шифруемый текст блоками по m x n - *s* элементов (m x n - размеры таблицы, *s* - число неиспользуемых элементов) записывается в таблицу. Далее процедура шифрования заключается в том, что текст выписывается по столбцам в последовательности цифр ключа.

Зашифрованный текст будет выглядеть так:

ДОПР*а* БСВИК РРТМ*а* ОЫ*а*На ЕНСЕФа УТ*а*ИС
С*а*АФИ*а* ЬОЕЕЫ*а* *а*ТМЕ*а* ТЖДЛ*а*

При расшифровании знаки зашифрованного текста записываются столбцами таблицы в последовательности знаков ключа с пропуском не-

используемых элементов. Исходный текст считывается по строкам.

Варьируя размерами таблицы, последовательностью символов ключа, количеством и расположением неиспользуемых элементов можно получить требуемую стойкость зашифрованного текста. Весьма высокую стойкость

шифрования можно обеспечить усложнением перестановок по маршрутам типа гамильтоновских. При этом для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного

текста считываются по маршрутам Гамильтона, причем используется несколько различных маршрутов. Для примера рассмотрим шифрование по маршрутам Гамильтона при $n = 3$. Структура и пять маршрутов показаны на рисунке 8, а пример шифрования - на рисунке 9.

Из рассмотренных примеров очевидно, что все процедуры шифрования и расшифровки па методу перестановок являются в достаточной степени формальными и могут быть реализованы алгоритмически.

Шифрование методам гаммирования. Суть метода гаммирования состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, ко-

торая называется гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название «гаммирование».

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k , где k - число символов в алфавите, т. е.

$t^{ш} = (t^0 + t^r) m^0 \, d^k$,

где $t_{ш}$, t_0 , t^r - символы соответственно зашифрованного, исходного текста и гаммы.

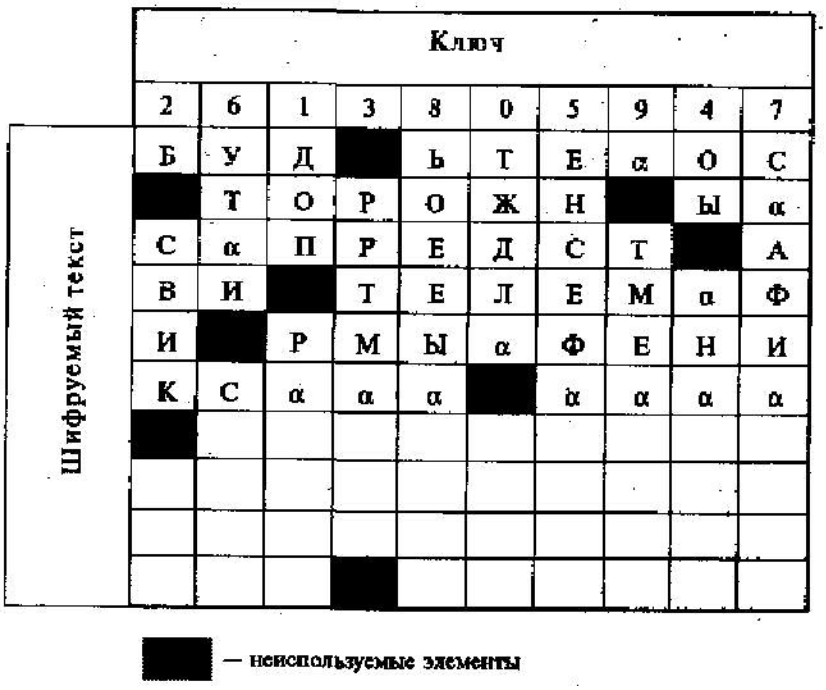


Рисунок 7 – Пример усложненной перестановки по таблице

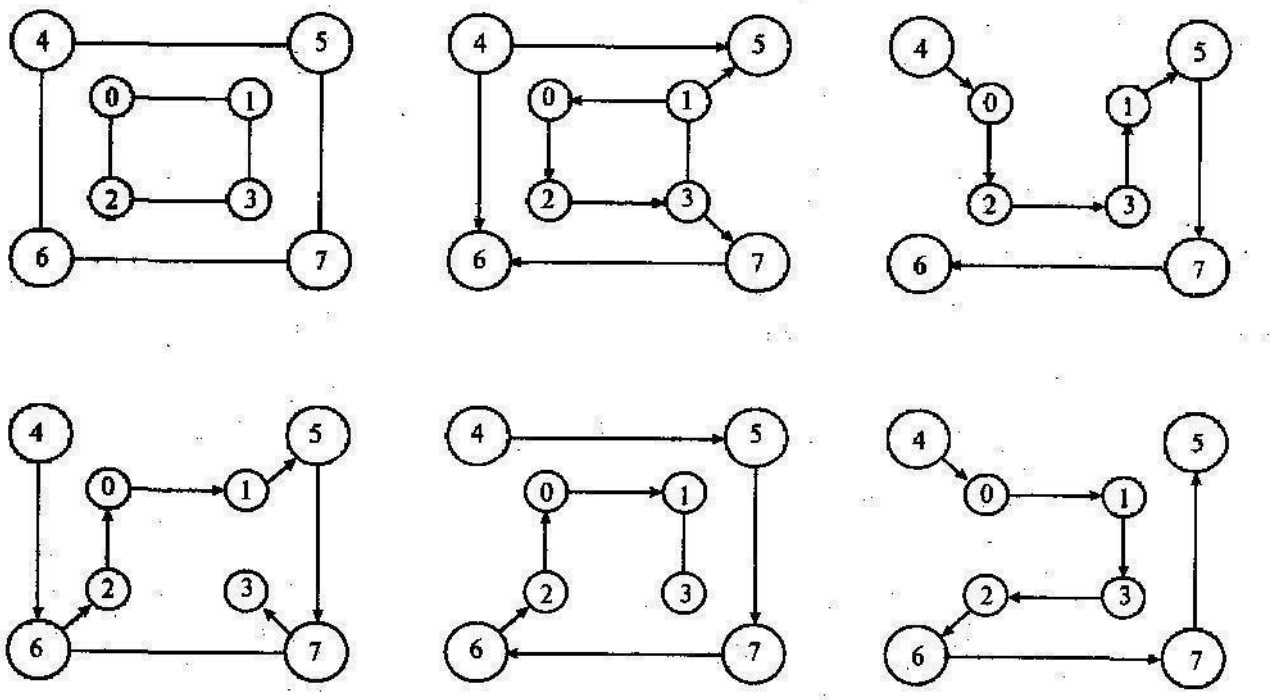


Рисунок 8 – Шифрование перестановкой по маршрутам

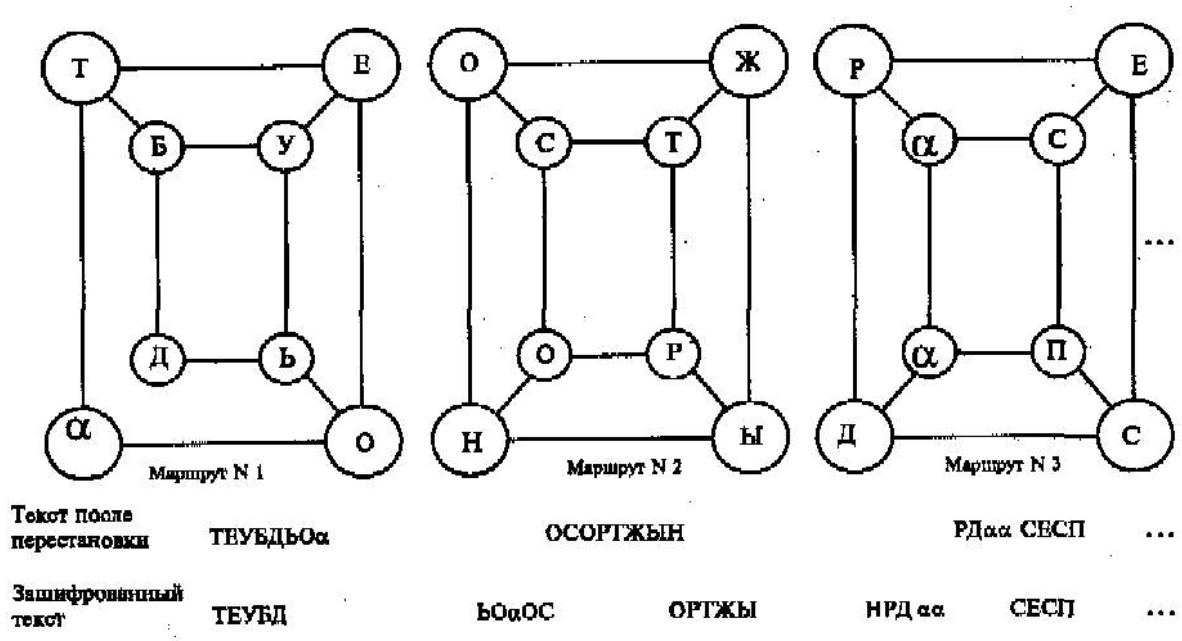


Рисунок 9 – Пример шифрования по маршрутам Гамильтона При втором методе символы исходного текста и гаммы представляются

в виде двоичного кода, затем соответствующие разряды складываются по модулю *2*. Вместо сложения по модулю 2 при гаммировании можно использовать и другие логические операции, например преобразование по правилу логической эквивалентности или логической неэквивалентности.

Такая замена равносильна введению еще одного ключа, которым является выбор правила формирования символов зашифрованного сообщения из символов исходного текста и гаммы. Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы -

длительностью периода и равномерностью статистических характеристик.

Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода.

Обычно разделяют две разновидности гаммирования - с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При

этом, если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т. е. его нельзя вскрыть при помощи статистической обработки зашифрованного текста. Это,

однако, не означает, что дешифрование такого текста вообще невозможно:

при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

В качестве гаммы может быть использована любая последовательность случайных символов, например, последовательность цифр числа π , числа e

(основание натурального логарифма) и т. п. При шифровании с помощью ЭВМ последовательность гаммы формируется с помощью датчика псевдослучайных чисел (ПСЧ). В настоящее время разработано несколько алгоритмов работы таких датчиков, которые обеспечивают удовлетворительные характеристики гаммы.

Шифрование с помощью аналитических преобразований. Достаточно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Для этого можно использовать методы алгебры матриц, например, умножение матрицы на вектор по правилу:

$$a_{ij} b_j = c_j = \sum a_{ij} b^j . {}^j$$

Если матрицу a^{ij} использовать в качестве ключа, а вместо компонента вектора b^j подставить символы исходного текста, то компоненты вектора c^j

будут представлять собой символы зашифрованного текста.

Приведем пример использования такого метода, взяв в качестве ключа квадратную матрицу третьего порядка

$$\begin{Vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{Vmatrix}.$$

Заменим буквы алфавита цифрами, соответствующими их порядковому

номеру в алфавите: А-0, Б-l, В-2, и т. д. Тогда отрывку текста ВАТАЛА... (текст взят произвольно) будет соответствовать последовательность 2, 0, 19,

0, 12, 0, По принятому алгоритму шифрования выполним необходимые действия:

$$\begin{vmatrix} 14 & 8 & 3 & 2 \\ 8 & 5 & 2 & . \\ 3 & 2 & 1 & \end{vmatrix} \begin{vmatrix} 0 \\ 19 \\ 0 \end{vmatrix} = \begin{vmatrix} 85 \\ 54 \\ 25 \\ 96 \end{vmatrix}$$

$$8\ 5\ 2\ .12 = 60\ .$$

$$3\ 2\ 1 \qquad\quad 0 \qquad 24$$

При этом зашифрованный текст будет иметь вид: 85, 54, 25, 96, 60, 24.

Расшифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве основы берется матрица,

обратная той, с помощью которой осуществляется закрытие, а в качестве вектора-сомножителя - соответствующее количество символов закрытого текста; тогда значениями вектора-результата будут цифровые эквиваленты знаков открытого текста.

Обратной к данной, как известно, называется матрица, получающаяся из так называемой присоединенной матрицы делением всех ее элементов на определитель данной матрицы. В свою очередь присоединенной называется матрица, составленная из алгебраических дополнений А, к элементам данной матрицы, которые вычисляются по формуле:

$$A_{ij} = (-1)^{i+j} D_{ij},$$

где D_{ij} - определитель матрицы, получаемый вычеркиванием 1-й ее строки *j*-го столбца. Определителем же, как известно, называется алгебраическая сумма *n!* членов (для определителя *n*-го порядка), составленная следующим образом: членами служат всевозможные произведения *n* элементов матрицы,

взятых по одному в каждой строке и в каждом столбце, при чем член суммы берется со знаком плюс, если его индексы составляют четную подстановку, и со знаком минус - в противном случае. Для матрицы третьего порядка, например, определитель вычисляется по следующей формуле:

$$D = A_{11}A_{22}A_{33} + A_{12}A_{23}A_{31} + A_{13}A_{21}A_{32} - A_{1123}A_{32} - A_{12}A_{21}A_{33} - A_{1322}A_{31}$$

Вычисленная по данной формуле матрица, обратная к принятой нами за основу для закрытия, будет иметь вид:

$$\begin{vmatrix} 1 & -2 & 1 \\ 2 & 5 & -4 \\ 1 & 44 & 6 \end{vmatrix}.$$

Тогда в условиях нашего примера процесс раскрытия будет выглядеть так:

$$\begin{vmatrix} 1 & -2 & 1 \\ 85 & 54 & 25 \end{vmatrix} = 1\cdot 85 - 2\cdot 54 + 1\cdot 25 = 2$$

$$\begin{vmatrix} -2 & 5 & -4 \\ 54 & 25 & 0 \end{vmatrix} = -2\cdot 85 + 5\cdot 54 - 4\cdot 25 = 0$$

$$\begin{vmatrix} 1 & -4 & 6 \\ 25 & 19 & 0 \end{vmatrix} = 1\cdot 96 - 4\cdot 54 + 6\cdot 25 = 19$$

$$\begin{vmatrix} 1 & -2 & 1 \\ 96 & 60 & 24 \end{vmatrix} = 1\cdot 96 - 2\cdot 60 + 1\cdot 24 = 0$$

$$\begin{vmatrix} -2 & 5 & -4 \\ 60 & 24 & 0 \end{vmatrix} = -2\cdot 96 - 5\cdot 60 - 4\cdot 24 = 12.$$

$$\begin{vmatrix} 1 & -4 & 6 \\ 24 & 1 & 0 \end{vmatrix} = 1\cdot 96 - 4\cdot 60 + 6\cdot 24 = 0$$

Таким образом, получили следующую последовательность шахов раскрытого текста: *2,* О, 19, 0, 12, 0, ..., что соответствует исходному тексту.

Нетрудно видеть, что и этот метод шифрования является формализованным, что позволяет легко реализовать его программными средствами.

Кодирование. Одним из средств криптографического закрытия информации, также имеющим длительную историю практического использования, является кодирование, под которым понимается замена элементов закрываемых данных некоторыми цифровыми, буквенными или комбинированными сочетаниями - копами. Нетрудно заметить, что между кодированием информации и ее шифрованием подстановкой и заменой

существует значительная аналогия. Однако между этими методами можно найти и различия.

При шифровании подстановкой заменяемыми единицами информации являются символы алфавита, и. следовательно, шифрованию могут подвергаться любые данные, для фиксирования которых используется

данный алфавит. При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования.

В общем случае необходимо использовать свою систему кодирования. Правда, в последнее время разработаны специальные коды, имеющие целью сократить объем информации при записи ее в ЗУ. Специфика этих кодов заключается в том, что для записи часто встречающихся символов используются короткие двоичные коды, а для записи редко встречающихся - длинные. Примером такого кода для английского языка может служить так называемый код Хаффмана, показанный на рисунке 10. Двоичный код для букв алфавита образуется путем последовательного выписывания нулей и единиц на маршруте от вершины графа до конца ветви, соответствующего данной букве. Тогда для варианта кода, представленного на рис. 6.15, буква £ кодируется комбинацией 001, R-1101, B-001110 и т. д. Если граф кодирования сохраняется в тайне, то такое кодирование имеет криптографическую стойкость на уровне шифрования простой заменой.

При смысловом кодировании основной кодируемой единицей является смысловой элемент текста. Для кодирования составляется специальная таблица кодов, содержащая перечень кодируемых элементов и соответствующих им кодов. Введем, например, следующую кодовую таблицу:

Автоматизированные системы управления	001
Автоматизация управления	002
Осуществляет	415
Позволяет	632

Тогда предложение «Автоматизированные системы управления

позволяют осуществлять автоматизацию управления» после кодирования будет иметь вид: 001 632 415 002.

Рассечение-разнесение данных состоит в том, что массив защищаемых данных рассекается на такие элементы, каждый из которых не позволяет

раскрыть содержание защищаемой информации, и выделенные таким образом элементы размещаются в различных зонах ЗУ. Обратная процедура называется сборкой данных. Совершенно очевидно, что алгоритм разнесения и сборки данных должен тщательно охраняться.

Пусть, например, текст, подлежащий закрытию, записан в поле ЗУ так,

как показано на рис. 6.16. Выберем блок данных длиною в восемь строк и разобьем его на элементы по две строки и два столбца в каждом. Для записи защищаемого текста требуется 16 зон ЗУ. Пусть строки блока перебираются

в последовательности 1-4-3-2, а столбцы в последовательности 2-4-3-1. Тогда

в *k*-ю зону ЗУ (*k=1,2,…,mn,* где *m*- число строк блока; *n* - число столбцов)

будет занесен элемент блока с номером

$$N_k = (r_i - 1)n + S_j,$$

где r_i – значение *i*-й позиции ключа строки; S_j – значение *j-й* позиции столбца.

Вычисленные по этой формуле значения будут следующими:

$N_1 = 2$ $N_5 = 14$ $N_9 = 10$ $N_{13} = 6$

$N_2 = 4$ $N_6 = 16$ $N_{10} = 12$ $N_{14} = 8$

$N_3 = 3$ $N_7 = 15$ $N_{11} = 11$ $N_{15} = 7$

$N_4 = 1$ $N_8 = 13$ $N_{12} = 99$ $N_{16} = 5.$

После такого разнесения текста, представленного на рисунке 11 содержание кодой из 16 зон ЗУ будет таким, как показано на рисунке 12.

Современные шифры – это сложная комбинация замен и перестановок.

Любое шифрпреобразование можно представить как последовательность операции, производимых с элементами ключа и открытого текста а также с производными от них величинами.

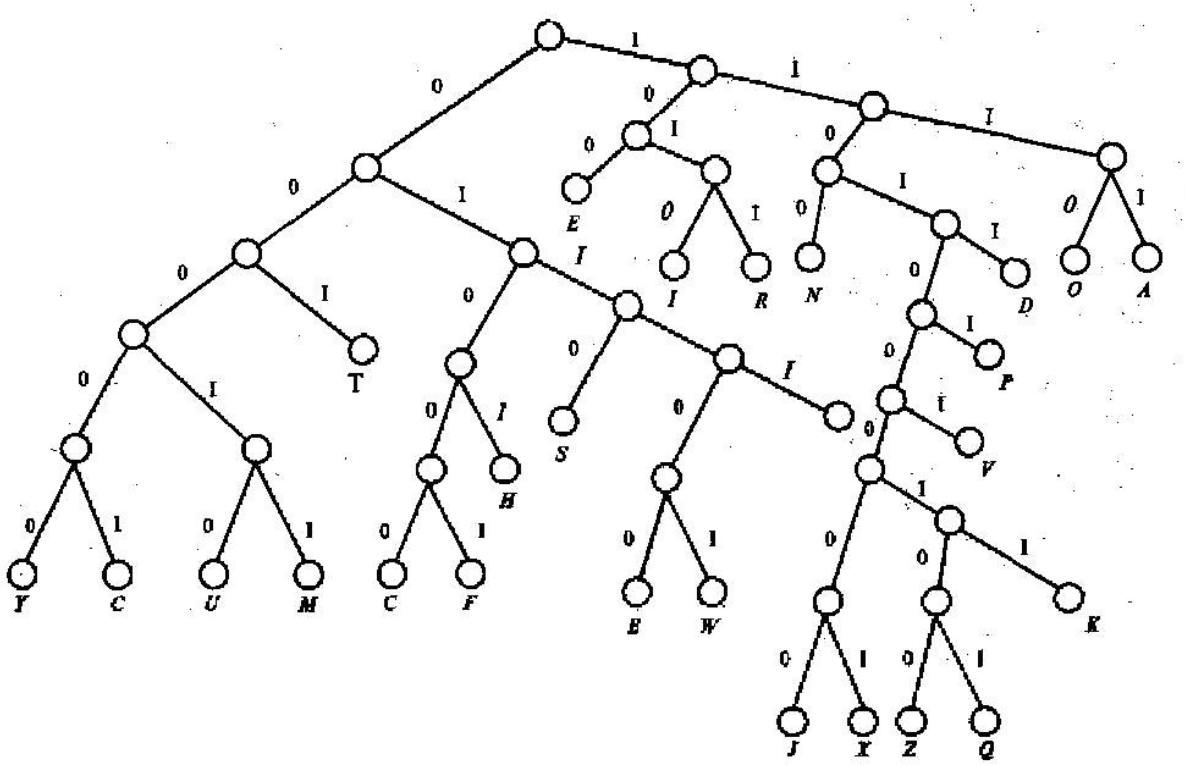


Рисунок 10 – Коды Хоффмана

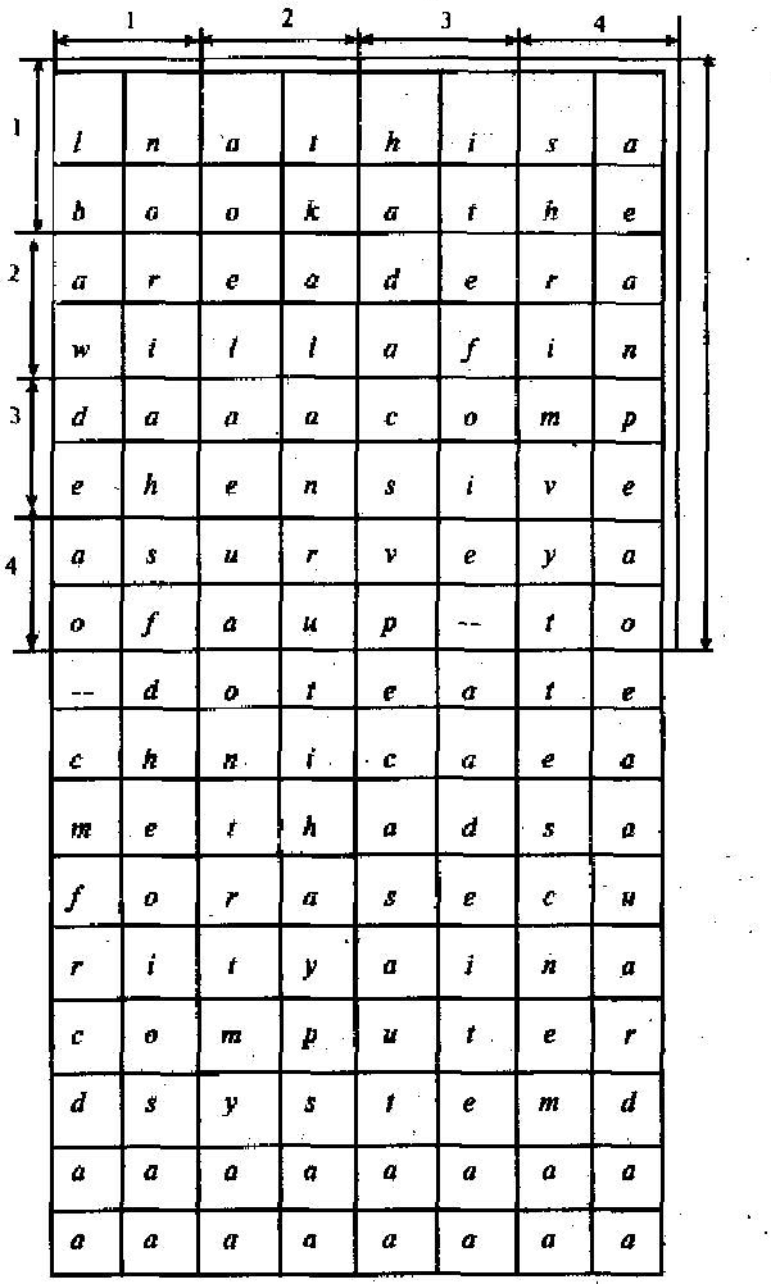


Рисунок 11 – Разбивка текста для закрытия методом рассечения -

разнесения Произвол в выборе элементов алгоритма шифрования достаточно

велик. В то же время, алгоритм шифрования не является абсолютно случайной последовательностью операций. Операции, используемые для построения алгоритмов шифрования (своего рода «элементная база»

шифров), должны обладать некоторыми хорошими криптографическими свойствами, как бы препятствовать тем или иным методам атаки на шифр, и кроме того, допускать удобную техническую или программную реализацию.

При построении хороших алгоритмов шифрования помимо выбора подходящих операции большое значение имеет конструирование взаимосвязей между элементами алгоритма. От особенностей соединения операций в последовательность, определяющую алгоритм шифрования зависит уровень практической стойкости шифра.

Рассмотрим подробнее широко известные алгоритмы блочного шифрования данных в США и России.

В 1973 г. Национальное бюро стандартов США начало разработку программы по созданию стандарта шифрования данных на ЭВМ. Был

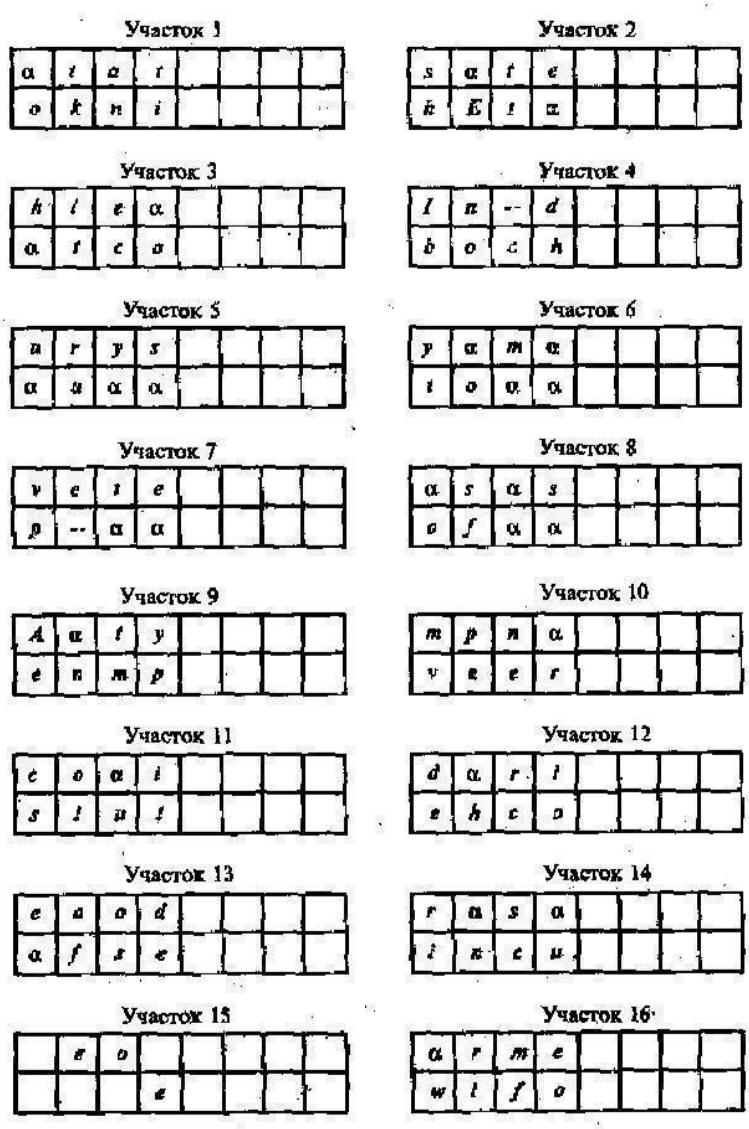


Рисунок 12 – Структура ЗУ с разнесенными данными

объявлен конкурс среди фирм-разработчиков США; который выиграла фирма IBM, представившая в 1974 г. алгоритм шифрования, известный под названием DBS (Data Encryption Stand art).

На рисунке 13 представлена блок-схема DES-алгоритма; Входные 64-битовые векторы, называемые блоками открытого текста, преобразуются в выходные 64-битовые векторы, называемые блоками шифртекста, с помощью двоичного 56-битового ключа *K.* Число различных ключей DES-алгоритма равно $2 \text{»} 7*10^{16}$.

Алгоритм реализуется в течение 16 аналогичных циклов шифрования, где на 1-м цикле используется цикловой ключ K_i, представляющий собой алгоритмически вырабатываемую выборку 48 битов из 56 битов ключа *K, i*= 1,2,…, 16.

На цикле шифрования производятся следующие операции с входными и ключевыми данными: E-расширение 32-битового вектора до 48-битового путем дублирований 16 битов, побитовое суммирование векторов, замена 6-битовых векторов на 4-битовые с помощью S-боксов S_1,..., S_8 , перестановка *P* битов 32-битового вектора.

Алгоритм обеспечивает высокую стойкость, однако недавние результаты показали, что современная технология позволяет создать вычислительное устройство стоимостью около 1 млн. долларов США, спо-собное вскрыть секретный ключ с помощью полного перебора в среднем за 3,5 часа.

Из-за небольшого размера ключа было принято решение использовать DES-алгоритм для закрытия коммерческой (несекретной) информации.

Лабораторная реализация перебора всех ключей в данных условиях экономически нецелесообразна, так как затраты на реализацию перебора не соответствуют ценности информации, закрываемой шифром.

DES-алгоритм явился первым примером широкого производства и внедрения технических средств в области защиты информации.

Национальное Бюро Стандартов США организовало проверку аппаратных

реализаций DES-алгоритма на специальном тестирующем стенде. Только после положительных результатов проверки производитель получает от Национального Бюро Стандартов сертификат на право реализации своего продукта. К настоящему времени аттестовано несколько десятков изделий,

выполненных на различной элементной базе.

Достигнута высокая скорость шифрования. По некоторым сообщениям,

имеется микросхема, реализующая DES-алгоритм со скоростью 45 Мбит/с.

Велика доступность этих изделий: стоимость некоторых аппаратных реализаций ниже 100 долларов США,

Основные области применения DES-алгоритма:

1) хранение данных в ЭВМ (шифрование файлов, паролей);

2) аутентификация сообщений (инея сообщение и контрольную группу, несложно убедиться в подлинности сообщения);

3) электронная система платежей (при операциях с широкой клиентурой и между банками);

4) электронный обмен коммерческой информацией (обмен данными между покупателем, продавцом и банкиром защищен от изменений и перехвата);

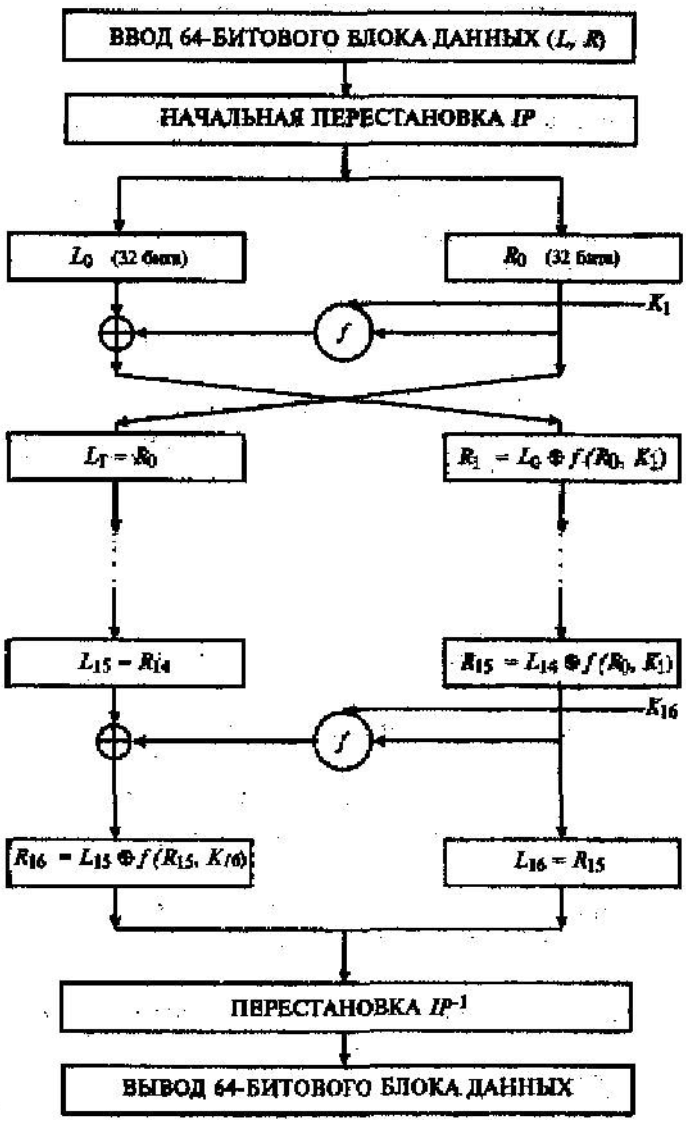


Рисунок 13– Блок-схема DES-алгоритма

В 1989 году в СССР был разработан блочный шифр для использования в качестве государственного стандарта шифрования данных. Разработка была принята и зарегистрирована как ГОСТ 28147-89. И хотя масштабы применения этого алгоритма шифрования до сих пор уточняются, начало его внедрению, в частности, в банковской системе, уже положено. Алгоритм,

судя по публикациям, несколько медлителен, но обладает весьма высокой стойкостью.

Блок схема алгоритма ГОСТ отличается от блок-схемы DES-алгоритма лишь отсутствием начальной перестановки и числом циклов шифрования (32

в ГОСТе против 16 в DES-алгоритме).

Ключ алгоритма ГОСТ - это массив, состоящий из 32-мерных векторов $X_1, X_2, \ldots, X_8$. Цикловой ключ 1-го цикла K_i, равен X_S, где ряду значений i от 1 до 32 соответствует следующий ряд значений s:

1,2, 3, 4, 5,6, 7, 8, 1, 2, 3, 4, 5,6,7, 8, 1, 2, 3, 4, 5, б, 7, 8, 8, 7,6, 5, 4, 3, 2,1.

Алгоритм расшифрования отличается от алгоритма зашифрования тем, что последовательность ключевых векторов используется в обратном порядке.

Расшифрование данных возможно только при наличии синхропосылки,

которая в скрытом виде хранится в памяти ЭВМ или передается по каналам связи вместе с зашифрованными данными.

Важной составной частью шифрсистемы является ключевая система шифра. Под ней обычно понимается описание всех видов ключей

(долговременные, суточные, сеансовые и др.), используемых шифром, и

алгоритмы их использования (протоколы шифрованной связи).

В электронных шифраторах в качестве ключей могут использоваться начальные состояния элементов памяти в схемах, реализующих алгоритм шифрования, функциональные элементы алгоритма шифрования. Ключ может состоять из нескольких ключевых составляющих различных типов;

долговременных, сеансовых и т. д.

Одной из основных характеристик ключа является его размер, определяющий число всевозможных ключевых установок шифра. Если размер ключа недостаточно велик, то шифр может быть вскрыт простым перебором всех вариантов ключей. Если размер ключа чрезмерно велик, то это приводят к удорожанию изготовления ключей, усложнению процедуры установки ключа, понижению надежности работы шифрующего устройства и т. д. Таким образом, выбранный криптографом размер ключа - это всегда некий компромисс.

Заметим, что DES-алгоритм подвергался критике именно в связи с небольшим размером ключа, из-за чего многие криптологии пришли к мнению, что необходимым «запасом прочности» DES-алгоритм не обладает.

Другой важной характеристикой ключа является его случайность. Наличие закономерностей в ключе приводит к неявному уменьшению его размера и,

следовательно, к понижению криптографической стойкости шифра. Такого рода ослабление криптографических свойств шифра происходит, например,

когда ключевое слово устанавливается по ассоциации с какими-либо именами, датами, терминами. Всякая логика в выборе ключа наносит ущерб криптографическим свойствам шифра.

Таким образом, требование случайности ключей выступает как одно из основных при их изготовлении.

Для изготовления ключей могут использоваться физические датчики и псевдослучайные генераторы со сложным законом образования ключа.

Использование хорошего физического датчика более привлекательно с точки зрения обеспечения случайности ключей, но является, как правило, более дорогим и менее производительным способом. Псевдослучайные генераторы более дешевы и производительны, но привносят некоторые зависимости если не в отдельные ключи, то в совокупности ключей, что также нежелательно.

Важной частью практической работы с ключами является обеспечение секретности ключа. К основным мерам по защите ключей относятся следующие:

1) ограничение круга лиц, допущенных к работе с ключами;

2) регламентация рассылки, хранения и уничтожения ключей;

3) регламентация порядка смены ключей;

4) применение технических мер защиты ключевой информации от несанкционированного доступа.

Важной составляющей защиты информации являются протоколы связи,

определяющие порядок вхождения в связь, зашифрования и передачи информации. Протокол связи должен быть построен с учетом следующих обстоятельств:

1) протокол должен защищать открытый текст и ключ от несанкционированного доступа на всех этапах передачи информации от источника к получателю сообщений;

2) протокол не должен допускать выхода в линии связи "лишней" информации, предоставляющей криптоаналитику противника дополнительные возможности дешифрования криптограмм.

Нетрудно видеть, что использование криптосистем с секретным ключом предполагает заблаговременные до сеансов связи договоренности между абонентами о сеансовых секретных ключах или их предварительную пересылку по защищенному каналу связи. ЕС настоящему времени разработаны принципы так называемого открытого распределения ключей

(ОРК) и открытого шифрования (ОШ), которые явились «новыми направлениям» в криптографии, давшим начало криптографии с открытым ключом.

Рассмотрим схему ОРК. В протоколе обмена секретными ключами предполагается, что все пользователи знают некоторое простое число p и примитивный элемент a(1<a<p) конечного поля GF(p) (то есть элемент,

степени которого a^t все ненулевые элементы поля *{1, 2,…, p-1}).* Такие

элементы всегда существуют, их число равно *j*(*j* (*p*)), функция Эйлера. Для выработки общего секретного ключа *k* пользователи A и B:

1) независимо друг от друга выбирают случайные числа k_A и k_B из интервала

(1,…. p-1), называемые секретными ключами пользователей;

2) вычисляют с использованием известных *p* и *a* величины:

$y^A = a^{k_A} \pmod p$ и $y^B = a^{k_B} \pmod p$,

которые являются открытыми ключами пользователей;

3) обмениваются ключами y_A и y_B по открытому каналу связи (с подтверждением их авторства, чтобы избежать замены их кем-то другим);

4) по полученным ключам $y_л$ и $y_в$ независимо вычисляют секретный параметр k, который и будет их общим сеансовый секретным ключом.

$$A : y^k A^{(\mathrm{mod}\ p)} = (a^{k_B})^{k_A} \mod p = a^{k_B k_A} \mod p = k$$

$$B$$

$$B : y^k A^{(\mathrm{mod}\ p)} = (a^{k_A})^{k_B} \mod p = a^{k_A k_B} \mod p = k$$

$$B$$

Развитие обозначенных подходов позволило разработать достаточно эффективные системы шифрования защищаемых данных и системы так называемой цифровой (электронной) подписи, обладающей основными свойствами собственноручной подписи человека.

Приведем однако пример, иллюстрирующий реальные возможности эффективного использования достаточно простых средств шифрования для обеспечения промышленной, торговой и другой тайны.

Пусть, например, руководство и агент (представитель) какого-либо предприятия (фирмы, концерна) договорились обмениваться закрытыми сообщениями, используя для этого шифр усложненной перестановки. С

целью повышения надежности закрытия подготовлено семь вариантов таблиц перестановки с «пустышками», каждая из которых снабжена своим ключом. Договорились также, что в каждый из дней недели будет использоваться соответствующая таблица. Один из возможных вариантов распределения таблиц приведен на рисунке 14. Пусть, например, руководство предприятия передает своему представителю указание следующего содержания: «Предложите партию в сто единиц по цене семьсот руб.»

Используя правила шифрования по данному методу, нетрудно убедиться, что в зависимости от дня недели данное сообщение будет представлено в таком виде:

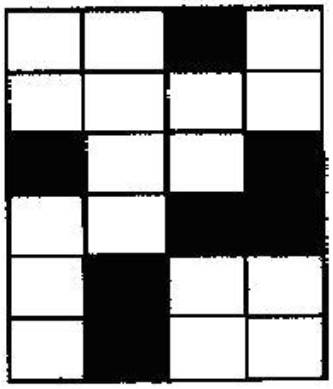
Понедельник: РЛИ*а*ОТАИПДБПТЕЖРЮВТЕНОДЦО*а*СН ИПааОаЕаМОСЬ*а*Б ЦЕСТУНЕР.

Вторник: РЛИРЮЮТТПЖ*а*АДЕПИВОЙЦЕСЕНЕ*а*Д ЦОТИПНЕ*а*МР. ЦСБУ ЦЕО*а*ЕСТБ,

Среда:ПДИПЮБРЮЖ*а*ТРЛТАИ*а*СЕИ*а*ОИ*ааа*НП ВТДЦОЦЕМТНССР. УОНУ*а*О*а*Б.

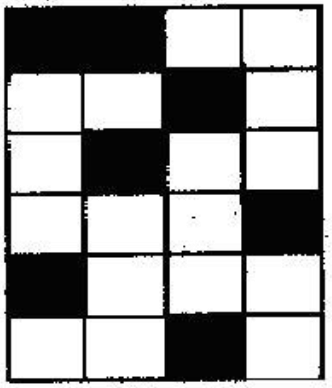
Понедельник

3 1 2 4



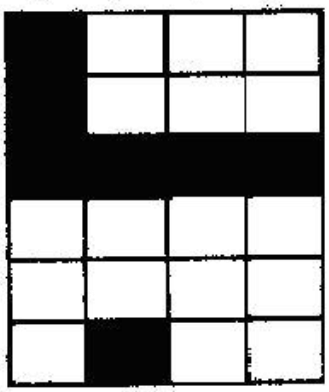
Вторник

2 4 3 1



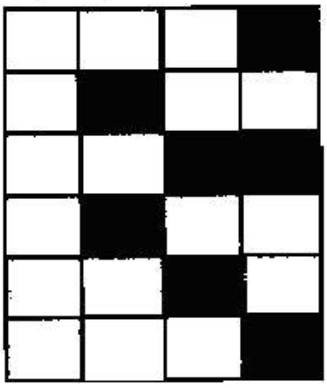
Среда

3 1 4 2



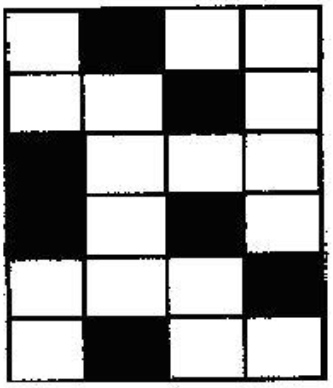
Четверг

1 3 4 2



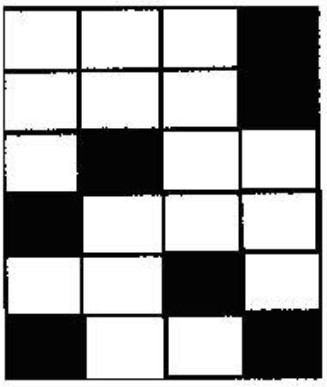
Пятница

3 2 1 4



Суббота

4 1 3 2



Воскресенье

4 3 1 2

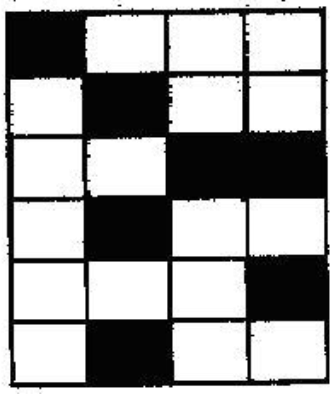


Рисунок 14 – Вариант использования таблиц усложненной замены

Предлагаем продолжить шифрование для остальных дней недели убедиться, что одной то же сообщение в каждый из дней недели шифруется различным образом, а если учесть, что сообщения типа рассмотренного выше должны сохраняться в тайне сравнительно непродолжительное время, то ясно, что рассмотренный в примере способ закрытия следует признать достаточно эффективным.

Аппаратура и материалы:

1. ПЭВМ

Методика и порядок выполнения работы

1. Ознакомиться с теоретическими сведениями, изложенными в данных методических указаниях

2. Рассмотреть основные требования к криптографическому закрытию информации

3. Рассмотреть укрупненную схему алгоритма шифрования по таблицеВижинера

4. Рассмотреть пример шифрования по маршрутам Гамильтона

5. Рассмотреть сущность и схему шифрования способом рассечения-разнесения.

6. Оформить отчет

Содержание отчета и его форма

Отчет должен иметь форму согласно оформлению простого реферата.

Титульный лист должен включать название дисциплины, название практической работы, фамилию и инициалы сдающего студента, номер группы, фамилию и инициалы принимающего преподавателя.

Основная часть практической работы должна содержать:

1. Описание возможностей применения криптографических методов
2. Основные требования к криптографическому закрытию информации

3. Классификацию криптографических методов преобразования информации

4. Описание простых систем криптографического преобразования

5. Укрупненную схему алгоритма шифрования по таблице Вижинера

6. Пример шифрования по маршрутам Гамильтона

7. Пример шифрования с помощью аналитических преобразований

8. Описание принципа открытого распределения ключей

9. Выводы по проделанной работе

Вопросы для защиты работы

1. Дайте определение и раскройте принципы построения криптографических средств защиты

2. Приведите и объясните классификацию методов криптографического преобразования информации

3. Раскройте сущность и схему шифрования заменой по таблице Вижинера

4. Раскройте сущность и схему шифрования перестановкой по таблице

5. Раскройте сущность и схему шифрования по маршрутам Гамильтона

6. Раскройте сущность и схему шифрования способом рассечения-разнесения.

Контрольные вопросы и задания для самостоятельной работы

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.

15. Проанализировать особенности угроз автоматизированным информационным системам.

16. Дать классификацию удаленных атак.

17. Проанализировать основные направления правовой защиты информации.

18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.

19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.

20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.

21. Определить объекты защиты авторских прав.

22. Назвать основные права автора в отношении его произведения.

23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).

25. Дать определение государственной тайны и назвать грифы секретности.

26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.

28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

30. Охарактеризовать порядок установления режима коммерческой

тайны и основные права ее субъектов.

31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.

32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

33. Назвать основные положения концепции информационной безопасности предприятия.

34. Изложить содержание регламента обеспечения информационной безопасности предприятия.

35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

42. Проанализировать особенности текста конфиденциального документа.

43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.

44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

45. Сформулировать возможности, трудности и направления использования
электронной почты для передачи конфиденциальных документов.

46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные
документы.

47. Проанализировать задачи защиты информации, которые должны быть
решены при формировании и оформлении дел с конфиденциальными документами.

48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.

49. Проанализировать пути поиска документов и дел, не обнаруженных при
проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.

51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. .

52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.

53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

54. Назвать основные элементы физической защиты территории и помещений предприятия.

55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.

56. Дать классификацию компьютерных вирусов.

57. Описать основные антивирусные программы.

58. Охарактеризовать основные способы криптографического преобразования данных.

Примерная тематика рефератов:

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность **(**по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

12. Составление инструкции по обработке и хранению конфиденциальных документов.

13. Направления и методы защиты документов на бумажных носителях.

14. Направления и методы защиты машиночитаемых документов.

15. Архивное хранение конфиденциальных документов.

16. Направления и методы защиты аудио- и визуальных документов.

17. Порядок подбора персонала для работы с конфиденциальной информацией.

18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

23. Порядок защиты информации в рекламной и выставочной деятельности.

24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для
обработки и хранения информации о конфиденциальных документах фирмы.
27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
28. Назначение, виды, структура и технология функционирования системы
защиты информации.
29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
30. Аналитическая работа по выявлению каналов утечки информации фирмы.
31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
32. Направления и методы защиты профессиональной тайны.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.
37. Защита секретов в дореволюционной России.
38. Методика инструктирования и обучения персонала правилами защиты
секретов фирмы.