**А.А. САРВИН**

**Л.И. АБАКУЛИНА**

**О.А. ГОТШАЛЬК**

# ДИАГНОСТИКА И НАДЕЖНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Письменные лекции

Санкт-Петербург

2003

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Государственное образовательное учреждение высшего профессионального образования

СЕВЕРО-ЗАПАДНЫЙ ГОСУДАРСТВЕННЫЙ ЗАОЧНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

**А.А. САРВИН Л.И. АБАКУЛИНА О.А. ГОТШАЛЬК**

# ДИАГНОСТИКА И НАДЕЖНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Утверждено редакционно издательским советом университета в качестве письменных лекций

Санкт-Петербург
2003

УДК 681. 5.004.52(075)
Сарвин А.А., Абакулина Л.И., Готшальк О. А. Диагностика и надежность автоматизированных систем: Письменные лекции. -СПб.: СЗТУ, 2003.- 69 с.

Письменные лекции соответствуют требованиям государственного образовательного стандарта высшего профессионального образования по направлению подготовки дипломированного специалиста 657900 – «Автоматизированные технологии и производства» (специальность 210200 – «Автоматизация технологических процессов и производств (в машиностроении)», специализация 210217 – «Компьютерные системы управления в производстве и бизнесе»).

В письменных лекциях изложены основы диагностирования и надежной работы технического и программного обеспечения автоматизированных систем управления технологическим оборудованием. Рассмотрены различные методы обеспечения диагностирования и надежности, направленные на сведение к минимуму возможных сбоев или нарушений в работе технологического оборудования от случайных или преднамеренных вмешательств в функционирование АСУ.

Письменные лекции включают материал, который читается в соответствии с рабочими учебными планами по дисциплине «Диагностика и надежность автоматизированных систем» студентам 5 курса специальности 210200 и специализации 210217.

Рецензенты: кафедра технологии автоматизированного машиностроения СЗТУ (заведующий кафедрой В.В.Максаров, д-р техн. наук, проф.); кафедра электротехники, вычислительной техники и автоматизации Санкт-Петербургского института машиностроения (завод – ВТУЗ) (заведующий кафедрой В.М.Шестаков, д-р техн. наук, проф.).

## ПРЕДИСЛОВИЕ

Под надежностью и безопасностью автоматизированной системы управления понимается ее защищенность от случайных или преднамеренных вмешательств в нормальный процесс ее функционирования, выражающийся в хищении или изменении информации (программная надежность), а также в нарушении ее работоспособности из-за отказов (аппаратная надежность).

Аппаратная надежность технических средств автоматизированных систем управления определяется свойствами, включающими в себя понятия безотказность, работоспособность, долговечность и сохраняемость.

Под программной надежностью и безопасностью автоматизированной системы управления понимается ее защищенность от случайных или преднамеренных вмешательств в нормальный процесс ее функционирования, выражающийся в хищении или изменении информации

Экономическая эффективность автоматизированной системы управления определяется уровнем ее аппаратной и программной надежности.

Снижение надежности приводит как вынужденным простоям, так и к аварийным ситуациям. Повышение надежности увеличивает стоимость системы и затраты на ее эксплуатацию.

Экономически целесообразный уровень надежности выбирается сравнением схожих по структуре и функциям вариантов (критерий оптимизации надежности).

## 1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Под автоматизированными системами управления (АСУ) понимается определенное количество компьютеров, промышленных контроллеров, устройств числового программного управления станками и промышленными роботами, устройств управления транспортными средствами и другими технологическими установками, объединенных локальными вычислительными

сетями и обеспечивающих сбор, обработку, хранение и передачу управляющей информации.

Под надежностью и безопасностью АСУ понимается ее защищенность от случайных или преднамеренных вмешательств в нормальный процесс ее функционирования, выражающийся в хищении или изменении информации, а также в нарушении ее работоспособности.

Случайные вмешательства:

- аварийные ситуации из-за стихийных бедствий или отключения электрического питания;
- отказы или сбои в работе электрических схем;
- ошибки в программировании;
- ошибки в работе обслуживающего персонала.

Преднамеренные вмешательства - это целенаправленные действия нарушителей.

Хищения связаны с разглашением конфиденциальной или секретной информации.

Изменение информации обусловлено ее искажением или уничтожением.

Нарушение работоспособности зависит либо от снижения производительности или функциональных возможностей, либо от блокировки доступа к некоторым информационным ресурсам АСУ.

Надежность технических средств системы определяется свойствами, включающими в себя понятия безотказность, работоспособность, долговечность и сохраняемость.

Безотказность – свойство системы сохранять свою работоспособность без вынужденных перерывов в течение некоторого периода времени, оцениваемого наработкой (длительность и объем выполненной работы до первого отказа).

Под работоспособностью понимается такое состояние системы, при котором она нормально выполняет заданные функции с заданными технической документацией параметрами.

Приспособленность системы к предупреждению, обнаружению и ликвидации отказов называется ремонтопригодностью.

Долговечность – свойство системы к длительной эксплуатации при необходимом техническом обслуживании и ремонте.

Долговечность системы измеряется ее ресурсом (наработка до предельного состояния) и сроком службы (календарная продолжительность эксплуатации до предельного состояния).

Предельное состояние системы определяется невозможностью ее дальнейшей эксплуатации по ряду причин:

- произошел отказ, после которого восстановление невозможно или нецелесообразно;
- по соображениям безопасности;
- из-за низкой экономической эффективности дальнейшего использования.

Под ремонтопригодностью понимается приспособленность системы к предупреждению, обнаружению и ликвидации отказов.

Ремонтопригодность характеризуется затратами времени и средств на восстановление системы после отказа и на поддержание системы в работоспособном состоянии.

Автоматизированные системы (АС) могут быть ремонтируемыми и неремонтируемыми.

Ремонтируемые системы имеют срок службы (ресурс), определяемый снижением эффективности работы системы и целесообразностью ее дальнейшей эксплуатации.

Неремонтируемыми являются системы, ремонт которых не возможен или не предусмотрен нормативно-технической, ремонтной или проектной документацией.

Под сохраняемостью понимается свойство системы (и составляющих ее элементов) сохранять свои параметры неизменными при определенных условиях (колебаниях температуры, действии влажности, вибрациях и т.п.) и сроках хранения и транспортировки.

***Вопросы для самоконтроля***

*1. К каким последствиям могут привести хищения, изменения или нарушения программного продукта АСУ?*

*2. Чем отличаются аппаратные нарушения работы АСУ от программных и какие могут быть последствия этих нарушений?*

*3. В чем отличие случайных от преднамеренных нарушений работы АСУ?*

## 2. КЛАССИФИКАЦИЯ ОТКАЗОВ

Важнейшим понятием теории надежности является понятие отказа.

Под отказом понимается событие, заключающееся в полной или частичной утрате работоспособности системы.

Отказ может быть связан с нарушением в выполнении каких-либо заданных функций (отказ функционирования) или с недостаточной квалификацией обслуживающего персонала, в результате которой система не выполняет заданные функции удовлетворительно. Отказы могут быть связаны с изменением параметров или характеристик системы, т.е. одна из основных функций выполняется плохо (отказ по параметру).

Классифицировать отказы можно в зависимости от характера и особенностей, от момента возникновения, например следующим образом [2].

1. По характеру изменения параметра до момента возникновения отказа:

- внезапный отказ;
- постепенный отказ.

2. По связи с другими отказами:

- независимый отказ;
- зависимый отказ.

3. По возможности последующего использования после возникновения отказа:

- полный отказ;
- частичный отказ.

4. По характеру устранения отказа:

- устойчивый отказ;
- самоустраняющийся отказ (сбой или перемежающийся отказ).

5. По наличию внешних проявлений:

- очевидный (явный) отказ;
- скрытый (неявный) отказ.

6. По причине возникновения:

- конструкционный отказ;
- технологический отказ;
- эксплуатационный отказ.

7. По природе происхождения:

- естественный отказ;
- искусственный отказ (вызываемый намеренно).

8. По времени возникновения отказов:

- отказ при испытаниях;
- отказ периода приработки;
- отказ периода нормальной эксплуатации;
- отказ последнего периода эксплуатации.

***Вопросы для самоконтроля***

1. *Что называется отказом в работе автоматизированной системы?*
2. *Чем отказ отличается от сбоя?*
3. *По какому принципу квалифицируются отказы?*

## 3. ПОКАЗАТЕЛИ НАДЕЖНОСТИ АСУ

Нарушение нормального выполнения заданных функций системы приводит к отказу в работе АСУ.

Функционирование АСУ – чередование интервалов работоспособности и отказов. Продолжительность этих интервалов – величина случайная. Поэтому

для описания показателей надежности АС используют математический аппарат теории вероятностей, теории случайных процессов и математической статистики. [1, 4]

Существует большое число показателей надежности АС. Рассмотрим те из них, которые определяются свойствами АС.

***Показатели безотказности***

Важнейшим показателем надежности ремонтируемых систем является величина *P(T)*, определяющая вероятность того, что наработка $T_H$ между отказами превзойдет заданное время *T*

$$P(T) = P(T_H \geq T).$$

Один из показателей безотказности - вероятность безотказной работы системы *P(t)*, т.е. вероятность того, что в течение времени (наработки) t не будет ни одного отказа, связана с вероятностью безотказной работы *F(t)*, т.е. вероятность того, что система откажет хотя бы один раз в течение заданной наработки, будучи работоспособной в начальный момент времени, простой зависимостью

$$P(t) = 1 - F(t).$$

Для экспоненциального закона распределения (одно из самых распространенных при исследовании надежности АСУ)

$$P(t) = e^{-\frac{t}{T_H}}.$$

Основными критериями безотказности ремонтируемых систем являются:

- вероятности наработки между отказами *P(t)* больше заданного значения *T*;
- параметр потока отказов системы (среднее число отказов системы за единицу времени) $\lambda = \sum_{i=1}^{r} N_i \lambda_i$, где $\lambda_i$ – интенсивность отказов;
- наработка на отказ (средняя продолжительность работы системы между двумя последовательными отказами) $T_H = 1/\lambda$;

- гарантированная (гамма-процентная) наработка до отказа, т.е. вероятность того, что в пределах заданной наработки отказ системы не возникает.

***Показатели ремонтопригодности***

Показателями ремонтопригодности являются:

- вероятность $P(T_З)$ восстановления системы за заданное время $T_З$;
- среднее время восстановления $T_В$ (определяет средние затраты времени на обнаружение и устранение отказа при заданных условиях обслуживания);
- гамма-процентное время восстановления – время, в течение которого восстановление работоспособности системы будет полностью осуществлено с вероятностью γ, выраженной в процентах;
- коэффициент готовности $k_Г$ - определяет вероятность того, что система исправна в любой произвольно выбранный момент времени в промежутках между плановым профилактическим обслуживанием и оценивается отношением времени наработки на отказ к средней длительности цикла работа-восстановление $k_Г = T_Н / (T_Н + T_В)$;
- коэффициент технического использования $k_{ТИ}$ - оценивается отношением времени наработки на отказ к средней длительности цикла работа-восстановление-профилактика $k_{ТИ} = T_Н / (T_Н + T_В + t_{пр})$.

***Показатели долговечности***

Долговечность системы характеризуется ее ресурсом $T_Р$ – общее время (или объем) работ системы за весь срок службы до момента, когда дальнейшая ее эксплуатация невозможна или экономически нецелесообразна;

Основными показателями долговечности системы являются:

- средний ресурс – математическое ожидание ресурса;
- гамма-процентный ресурс – суммарная наработка, в течение которой система не достигает предельного состояния с вероятностью γ, выраженной в процентах;

- гамма-процентный срок службы – календарная продолжительность эксплуатации, в течение которой система не достигнет предельного состояния с вероятностью γ, выраженной в процентах.

***Показатели сохраняемости***

Показатели сохраняемости дают количественную характеристику способности системы (и ее элементов) сохранять свое качество при хранении и транспортировке. Ее основными показателями являются:

- средний срок сохраняемости (среднее время хранения, в течение которого изменения параметров системы или ее элементов не превышают допустимых);
- гарантированный (гамма-процентный) срок сохраняемости, т.е. срок сохраняемости, достигаемый с заданной вероятностью γ, выраженной в процентах.

Нормальное функционирование АС зависит от действия составляющих ее элементов, т.е. вероятность безотказной работы системы зависит от вероятностей безотказной работы элементов системы $P_i(t)$ и определяется по формуле

$$P(t) = \prod_{i=1}^{N} P_i(t),$$

где $N$ – количество элементов.

Для обеспечения надежной работы всей системы вводится понятие избыточности системы.

Разделяют структурную и информационную избыточность.

Структурная избыточность определяется наличием дополнительных путей передачи сигналов (при отказе одного из элементов его функции выполняет другой элемент), которые не востребованы при нормальной работе.

Информационная избыточность определяется наличием в сигнале дополнительной информации, которая не востребована при нормальной работе всех элементов, а лишь при возникновении отказа.

Введение избыточности увеличивает надежность системы за счет повышения безотказности [1].

Повышение ремонтопригодности достигается применением унифицированных блочных конструкций, устройств диагностики и индикации отказов.

Надежность АСУ в основном определяется сочетанием свойств безотказности и ремонтопригодности.

***Вопросы для самоконтроля***

1. *Что называется работоспособным состоянием системы?*
2. *Назовите основные показатели надежности ремонтируемых систем.*
3. *Что понимается под структурной и информационной избыточностью системы?*

## 4. АНАЛИЗ НАДЕЖНОСТИ АСУ В ПРОЦЕССЕ ПРОЕКТИРОВАНИЯ

Для обеспечения необходимого уровня надежности АСУ в процессе проектирования, необходимо определить показатели надежности и разработать мероприятия по ее повышению [1, 4].

Для анализа надежности используют математические модели, которые учитывают свойства процессов функционирования реальной системы и ее элементов.

Основными методами анализа надежности в процессе проектирования являются: по среднегрупповым значениям интенсивностей отказов; с использованием данных эксплуатации; коэффициентный метод. Эти методы базируются на экспоненциальном распределении (модель отказов элементов и система), как наиболее распространенные при исследовании АСУ [1].

***Метод расчета надежности по среднегрупповым значениям интенсивностей отказов***. Исходными данными являются средняя (по числу элементов системы данной группы i) интенсивность отказов $\lambda_i$ и количество этих элементов $N_i$ в системе. Диапазон возможной интенсивности отказов $\lambda_i$ выбирается из таблиц литературных источников. Если система разбита на m групп с примерно одинаковыми интенсивностями отказов, то параметр потока отказов определяется по формуле

$$\lambda = \sum_{i=1}^{r} N_i \lambda_i \ ,$$

а наработка на отказ

$$T_H = 1 \diagup \lambda \ .$$

***Метод расчета надежности с использованием данных эксплуатации.***

При расчете надежности этим методом используют статистические данные о надежности АСУ, аналогичных по конструкции и назначению. Расчет надежности данным методом имеет в свою очередь две разновидности.

1) *По среднему уровню надежности однотипных систем*. Считается известным: количество элементов аналога $N_a$; количество элементов проектируемой системы $N_п$; наработка на отказ системы-аналога $T_{на}$ и $\lambda_{ai} = \lambda_{пi}$ ($\lambda_{ai}$ – средняя интенсивность отказов системы-аналога; $\lambda_{пi}$ - средняя интенсивность отказов проектируемой системы). Тогда наработка на отказ проектируемой системы определяется по формуле

$$T_{нп} = \frac{N_a}{N_n} T_{на} \ ,$$

а параметр потока отказов по формуле

$$\lambda_n = 1 \diagup T_{нп} \ . \qquad (1)$$

2) *С использованием коэффициентов пересчета в соответствии с реальными условиями эксплуатации*. Коэффициент пересчета определяется

$$a = T'_{на} \diagup T_{на} \ ,$$

где $T_{на}$ – расчетная наработка на отказ системы-аналога; $T'_{на}$ – опытная наработка на отказ системы-аналога.

$T_{на}$ определяется по табличным значениям интенсивностей отказов $\lambda_i$

$$T_{на} = \left( \sum_{i=1}^{r=1} N_{ia} \lambda_i \right)^{-1} .$$

Наработка на отказ проектируемой системы определяется

$$T_{нп} = aT_{на} ,$$

а параметр потока отказов по формуле (1).

***Коэффициентный метод***. Исходными данными для расчета являются: число элементов $N_i$, в системе, интенсивность отказов базового элемента $\lambda_б$, интенсивность i-го элемента $\lambda_i$. Тогда параметр потока отказов определяется по формуле

$$\lambda = \lambda_б \sum_{i=1}^{r} N_i k_i ,$$

где $k_i$ – коэффициент надежности, определяемый по формуле

$$k_i = \lambda_i / \lambda_б .$$

Коэффициентный метод является наиболее простым для расчета надежности и обладает наиболее высокой степенью точности.

Как отмечалось выше, рассмотренные методы позволяют оценить надежность на стадии проектирования. Более достоверно можно оценить надежность только на стадии эксплуатации.

### *Вопросы для самоконтроля*

1. *Перечислите основные методы для расчета надежности.*
2. *Какой из методов расчета надежности является наиболее точным?*

## 5. ЭФФЕКТИВНОСТЬ АСУ

Экономическая эффективность АСУ определяется уровнем надежности системы.

Снижение надежности приводит к возрастанию потерь при отказах. Повышение надежности – увеличивает стоимость системы и затраты на ее эксплуатацию.

Экономически целесообразный уровень надежности выбирается сравнением схожих по структуре и функциям вариантов (критерий оптимизации надежности) [1].

Под экономически целесообразным уровнем надежности понимается наилучший вариант по максимуму эффективности, измеряемой годовым дополнительным экономическим эффектом.

Т.е.

$$Э_Н = \left(\Delta C_П - E_Н \Delta k\right) \to \max,$$

где $\Delta C_П$ – годовая экономия от снижения себестоимости изготовления продукции при внедрении проектируемой системы;

$E_Н$ – нормативный коэффициент эффективности капиталовложений;

$E_Н \Delta k$ – нормативная экономия от использования дополнительных капиталовложений.

В качестве критерия оптимизации надежности часто используют величину дополнительного эффекта за срок службы системы $T_{сл}$

$$Э_T = \left(\Delta C_Д T_Э - \Delta k\right) \to \max, \qquad (2)$$

где $\Delta C_Д T_Э$ – экономия за счет понижения себестоимости $\Delta C_Д$ (без учета амортизационных отчислений);

$\Delta k$ – дополнительные капитальные затраты, от которых экономия получена;

$T_Э$ – эквивалентный срок службы.

$T_Э$ определяется по формуле:

$$T_Э = \left(1 - e^{-E_Н T_{сл}}\right) \Big/ E_Н .$$

Надежность системы будет оптимальной, если каждый элемент системы будет иметь оптимальную интенсивность $\lambda_{iopt}$ . Интенсивность отказов всей системы определяется по формуле:

$$\lambda_{opt} = \sum_{i=1}^{N} \lambda_{iopt} .$$

Дополнительный экономический эффект при этом будет наибольшим за счет снижения среднего числа отказов.

Пусть $\lambda_И$ – интенсивность исходной системы; $\lambda_П$ – интенсивность проектируемой системы и $\lambda_И > \lambda_П$.

Годовая экономия на расходах по эксплуатации при использовании проектируемой системы вместо исходной будет

$$\Delta C_{ДЭ} = C_{ВИ}\lambda_И - C_{ВП}\lambda_П,$$

где $C_В$ – средняя стоимость восстановления системы после отказов.

Если отказы обусловлены только отказами i-го элемента системы, то годовая экономия на расходах по эксплуатации, обусловленная повышением надежности элемента от $\lambda_И$ до $\lambda_П$ вычисляется по формуле

$$\Delta C_{ДЭ} = \Delta C_{ДЭi} = C_{Bi} (\lambda_И - \lambda_П) = C_{Bi} (\lambda_{Иi} - \lambda_{Пi}),$$

где $C_{Bi}$ – средняя стоимость восстановления i-го элемента (примерно одинаковая для обеих систем).

Потери от простоев

$$П = (В T_В + H) \lambda,$$

где В – условно-постоянные расходы в единицу времени;

$H$ – средний ущерб от одного отказа системы;

$T_В$ – среднее время восстановления каждого отказа.

Годовая экономия от сокращения потерь, вызванных простоями системы определяется разностью потерь от простоев исходной и проектируемой систем

$$\Delta C_{ДП} = П_И – П_П = В(T_{ВИ} \lambda - Т_{ВП}\lambda) + H(\lambda_И - \lambda_П).$$

Если отказы системы обусловлены только отказами i-го элемента со средним временем восстановления $T_{Bi}$, то

$$\Delta C_{ДП} = \Delta C_{ДПi} = (В T_{Bi} + H_i)(\lambda_{Иi} - \lambda_{Пi}).$$

$$\Delta C_{Дi} = \Delta C_{ДЭi} + \Delta C_{ДПi} = (В T_{Bi} + H_i + C_{Bi}) (\lambda_{Иi} - \lambda_{Пi}) = R_i (\lambda_{Иi} - \lambda_{Пi}),$$

где $R_i = (В T_{Bi} + H_i + C_{Bi})$.

Приращение стоимости элемента определяется

$$\Delta k_i' = S_i' \ln \frac{\lambda_{ui}}{\lambda_{Пi}},$$

где $S_i'$ - постоянная затрат на повышение надежности элемента, численно равна приращению стоимости элемента при снижении интенсивности отказов в e≈2,7 раза.

Подставим значения $\Delta k_i'$ и $\Delta C_{Дi}$ в формулу (2)

Получим

$$Э_{Ti} = (\lambda_{Иi} - \lambda_{Пi}) R_i T_Э - S_i' \ln \frac{\lambda_{Иi}}{\lambda_{Пi}}. \quad (3)$$

Если эквивалентные сроки службы элемента $T_{Эi}$ и системы не совпадают, то

$$Э_{Ti} = (\lambda_{Иi} - \lambda_{Пi}) R_i T_Э - S_i \ln \frac{\lambda_{Иi}}{\lambda_{Пi}},$$

где $S_i = S_i' \frac{T_Э}{T_{Эi}}$.

Из формулы (3) следует, что при повышении надежности элемента (уменьшении $\lambda_{Пi}$) эффект сначала возрастает, а затем снижается, т.е. существует максимум $Э_{Timax}$ . Это объясняется тем, что при высоком уровне надежности элемента затраты на дальнейшее ее повышение превышают получаемую при этом экономию на потерях, которая при высоком уровне надежности будет невелика.

Для определения оптимальной интенсивности отказов $\lambda_{iopt}$ необходимо продифференцировать по $\lambda_{Пi}$ выражение для $Э_{Ti}$ и приравнять производную нулю:

$$dЭ_{Ti} / d\lambda_{Пi} = -R_i T_Э + S_i / \lambda_{Пi} = 0,$$

откуда $\lambda_{Пiopt} = S_i / (R_i T_Э)$.

Тогда можно определить

$$Э_{Ti\max} = \left(\lambda_{Ии} - \lambda_{Пiopt}\right) R_i T_Э - S_i \ln \frac{\lambda_{Ии}}{\lambda_{Пiopt}} , \qquad (4)$$

и

$$\Delta k'_{iopt} = S'_i \ln \frac{\lambda_{Ии}}{\lambda_{Пiopt}} .$$

Зная $\lambda_{Пiopt}$ , определяем оптимальную интенсивность всей системы $\lambda_{opt}$ .

Экономический эффект от повышения надежности всей системы и необходимые для этого затраты равны

$$Э_{TC\max} = \sum_{i=1}^{N} Э_{Ti\max}$$

и

$$\Delta k_{Copt} = \sum_{i=1}^{N} \Delta k'_{iopt} .$$

### *Вопросы для самоконтроля*

1. *Какой уровень надежности считается экономически целесообразным?*
2. *Как объяснить, что при повышении надежности экономический эффект сначала возрастает, а затем снижается?*

## 6. МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ АСУ

При выборе способа повышения надежности функциональных элементов АСУ следует выбирать способ, при котором максимальный дополнительный экономический эффект $Э_{Тimax}$ будет наибольшим [1].

В формулу (4) введем обозначение

$$\lambda_{Ии} \Big/ \lambda_{iopt} = \lambda_{Ии} R_i T_Э \Big/ S'_i = Y_i ,$$

где $Y_i$ характеризует оптимальную меру повышения надежности элемента.

Тогда

$$Э_{Ti\max} = \lambda_{Ии} R_i T_Э \left[1 - \left(1 + \ln Y_i\right)/Y_i\right].$$

Наибольшее значение $Э_{Timax}$ будет при наибольшем $Y_i$ или наименьшем значении $S_i = (S_i T_Э)/T_{Эi}$ . Т.е. функциональный элемент системы имеет более высокую надежность, если

$$S_i'/T_{Эi} \to \min .$$

Существует ограниченное число методов повышения надежности АС, которые можно разделить на четыре группы.

1. Введение избыточности (внутриэлементной, структурной, информационной, алгоритмической) системы. Структурная избыточность (фактически – резервирование) позволяет создать надежные АС из ненадежных элементов.

2. Применение более надежных компонентов. Т.е. при разработке АС применяются элементы, которые выполняют требуемые функции в заданных условиях, но при сопоставлении, имеют более высокие показателями надежности.

3. Улучшение условий эксплуатации системы. Т.е. в процессе установки системы должна быть правильно выбрана компоновка элементов системы в блоках и обеспечен отвод тепла, выделяющегося при работе.

4. Организация интенсивного профилактического обслуживания системы и отдельных ее элементов.

Первые две группы реализуются на этапе разработки системы, а другие две – на этапе эксплуатации [1].

При сопоставлении показателей надежности ряда элементов, выполняющих требуемые функции в заданных условиях эксплуатации, выбираются элементы с более высокими показателями надежности. Это является наиболее эффективным способом повышения надежности всей системы.

Отдельно решается вопрос надежности систем при переходе от структурного к алгоритмическому принципу построения АС. Это приводит и к необходимости обеспечения надежности программных средств АС.

***Вопросы для самоконтроля***

*1. Перечислить методы повышения надежности АСУ.*

*2. При каком условии экономический эффект системы в течение срока службы будет оптимальным?*

## 7. РЕЗЕРВИРОВАНИЕ АСУ

Для создания надежных АСУ из недостаточно надежных элементов вводится понятие резервирования [1, 2].

Резервирование – способ обеспечения надежности за счет использования дополнительных средств и (или) возможностей, избыточных по отношению к минимально необходимым для выполнения требуемых функций.

Резервирование бывает общим (резервируется система в целом) и раздельным (система резервируется по узлам, блокам и элементам). Резервирование разделяется на постоянное и резервирование замещением в зависимости от способа включения избыточных элементов. При постоянном резервировании резервные элементы присоединены в течение всего времени работы. При резервировании замещением резервные элементы включаются в работу только в случае отказа основных элементов.

Основным параметром резервирования является его кратность

$$m = {(l-h)}/{h} \ ,$$

где $l$ – общее число элементов резервированного устройства;

$h$ – число резервируемых элементов, необходимых для нормальной работы устройства;

$l$-$h$ – число резервных элементов.

При общем резервировании система представляет собой цепочку из $N$ элементов.

Вероятность безотказной работы определяется

$$P(t) = \prod_{i=1}^{N} P_i(t),$$

где $P_i(t)$ – вероятность безотказной работы $i$ –го элемента в течение времени $t$.

При условии равнонадежности основных и резервных элементов при кратности $m$, вероятность безотказной работы резервированной системы будет

$$P_C(t) = 1 - [1 - P(t)]^{m+1}.$$

Вероятность отказа резервированной системы составит

$$Q_C(t) = 1 - P_C(t) = [1 - P(t)]^{m+1}.$$

При постоянных значениях интенсивности отказов элементов и параметра отказов цепочки $\lambda_0 = \sum_{i=1}^{N} \lambda_i$

$$P_C(t) = 1 - \left(1 - e^{-\lambda_0 t}\right)^{m+1}$$

и

$$Q_C(t) = \left(1 - e^{-\lambda_0 t}\right)^{m+1}$$

При раздельном резервировании вероятность безотказной работы и вероятность отказа при $m$-кратном резервировании равнонадежных элементов будут

$$P_C(t) = \prod_{i=1}^{N} \left\{ 1 - [1 - P_i(t)]^{m+1} \right\},$$

$$Q_C(t) = 1 - \prod_{i=1}^{N} \left\{ 1 - [1 - P_i(t)]^{m+1} \right\}.$$

При постоянном резервировании критерий эффективности определяется следующим образом

$$W_Q = Q_C(t) \big/ Q_H(t),$$

где $Q_C(t)$ - вероятность отказа исходной системы.

Выигрыш в надежности при общем постоянном резервировании будет

$$W_Q = \left(1 - e^{-\lambda_0 t}\right)^m.$$

Выигрыш в надежности при поэлементном постоянном резервировании N равнонадежных элементов будет

$$W_Q = \frac{1-\left(1-\left(1-e^{-\lambda t}\right)^{m+1}\right)^N}{1-e^{-N\lambda t}},$$

где λ – интенсивность отказов.

Постоянное резервирование преимущественнее других видов резервирования.

Существенное преимущество постоянного резервирования состоит в простоте выполнения (не требуются устройства обнаружения неисправностей и переключающие устройства, которые снижают общую надежность системы).

Резервирование замещением является наиболее эффективным. Но использование при таком резервировании переключающих элементов, делает целесообразным применять его только при повышении надежности крупных блоков узлов и микромодулей высокой степени интеграции.

Выбор вида резервирования для повышения надежности, как отдельного элемента, так и всей системы может быть сделан после тщательного анализа [1].

***Вопросы для самоконтроля***

1. *Что называется резервированием АСУ?*
2. *Какие виды резервирования АСУ существуют?*
3. *Какими преимуществами обладают различные виды резервирования?*

## 8. ТЕХНИЧЕСКАЯ ДИАГНОСТИКА АСУ. АЛГОРИТМЫ И МЕТОДЫ ДИАГНОСТИРОВАНИЯ

Одним из важнейших средств обеспечения и поддержания надежности АСУ является техническая диагностика.

Под технической диагностикой понимается область знаний, разрабатывающая методы и средства поиска отклонений в режимах работы

(или состояниях) АС, обнаружения и устранения дефектов в системах (или ее элементах) и средства их локализации.

При диагностировании необходимо определить, прежде всего, техническое состояние системы в данный момент времени [7]. Это означает, что нужно проверить исправность, работоспособность и (или) правильность функционирования системы (определить, находятся ли значения параметров системы в требуемых пределах, т.е. система не отказала и правильно выполняет заданную функцию) или обнаружить дефекты, нарушающие исправность, работоспособность и правильное функционирование системы. Тогда основную цель диагностирования АСУ можно сформулировать следующим образом: необходимо оценить выходные параметры системы и выявить причины их отклонения от заданных значений. При этом необходимо учитывать весь диапазон режимов работы системы и условий ее эксплуатации, а также возможность изменения выходных параметров во времени (так называемая параметрическая надежность).

Различают тестовое и функциональное диагностирование.

Тестовое диагностирование позволяет проверить техническое состояние системы по тестовому воздействию на нее. По тесту проверяются параметры системы и ее элементов и причины их отклонения от заданных значений.

Функциональное диагностирование позволяет определить техническое состояние системы (или ее элементов) по рабочему воздействию на нее. Рабочее воздействие контролирует исполнение системой заданных функций при заданных параметрах и выявить причины нарушения ее функционирования.

Тестовое и функциональное диагностирование выполняется по так называемому алгоритму диагностирования.

Алгоритм диагностирования – совокупность элементарных проверок в контрольных точках системы и правил, устанавливающих последовательность их проведения, а также анализ результатов этих проверок, по которым можно определить исправное, работоспособное или состояние правильного

функционирования от неисправного состояния и уметь отличать дефекты от неисправного состояния.

В алгоритмах тестового диагностирования контрольные точки определены предварительно и они одинаковы для всех проверок и подбираются только тестовые воздействия.

В алгоритмах функционального диагностирования предварительно определены входные воздействия, а выбору подлежат контрольные точки.

При проведении различных элементарных проверок могут требоваться различные затраты на их реализацию. Эти проверки могут давать разную информацию о техническом состоянии системы. Одни и те же элементарные проверки могут быть реализованы в различной последовательности. Т.е. для решения даже одной задачи диагностирования, можно построить несколько алгоритмов. Таким образом, встает задача разработки оптимальных алгоритмов диагностирования, при которых затраты на их реализацию будут уменьшены (задача минимизации в некоторых случаях может быть сильно затруднена, например, трудностями вычислений).

Эффективность диагностирования оценивается качеством алгоритмов диагностирования и качеством средств диагностирования. Средства диагностирования разделяют, прежде всего, на программные и аппаратные, а также внешние (конструктивно выполненные отдельно от системы) и встроенные (являющиеся составной частью системы); ручными, автоматизированными и автоматическими; специализированными и универсальными.

Методы диагностирования АСУ определяются различными факторами: выбором объекта диагностирования (узла, блока, элемента и т.п.), используемыми диагностическими параметрами (временные, силовые, электрические, виброакустические и др.), в зависимости от используемых средств диагностирования.

Широко применяется при диагностировании метод контрольных осциллограмм. Метод основан на использовании графиков функций различных

параметров во времени, по которым оцениваются техническое состояние и работоспособность отдельных узлов, блоков и системы в целом [7].

Суть метода заключается в следующем. Составляют диагностическую модель, определяют диагностическую ценность разных параметров, оценивают трудоемкость использования параметров для диагностирования, предварительно определяют диагностические параметры, экспериментально проверяют чувствительность к дефектам и диагностическую ценность параметров, выбирают основные диагностические параметры для контрольной осциллограммы, определяют внешний вид и характерные особенности кривых выбранных параметров, амплитудные значения и допустимые пределы для кривых основных параметров, составляют и экспериментально проверяют контрольные осциллограммы, выявляют взаимосвязь между характерными признаками кривых и состоянием обследуемых объектов, накапливают и расшифровывают дефекты, составляют диагностические карты и инструкции для выполнения диагностирования.

Метод контрольных осциллограмм может быть реализован как средствами приборной диагностики, так и с помощью ЭВМ в автоматическом режиме. Использовать метод целесообразно также на специализированных испытательных стендах для контроля качества изготовления механизмов и узлов станков и в условиях эксплуатации.

Эффективность процессов диагностирования во многом определяется программными средствами системы.

### *Вопросы для самоконтроля*

1. *Что входит в понятие техническая диагностика?*
2. *Назовите виды диагностирования и их отличительные особенности.*
3. *Назовите основные методы диагностирования.*

# 9. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ПРОГРАММНОЙ НАДЕЖНОСТИ АСУ

Построение надежных АСУ включает комплекс мер, направленных на защиту ее от случайных или преднамеренных воздействий, которые могут повлечь нарушение запрограммированного процесса управления.

Комплекс мер состоит из:

-правовых норм;

-морально-этических норм;

-административно-организационных мер;

-программно-технических средств.

1. Правовые нормы базируются на законах, указах, нормативных актах, регламентирующих правила обращения с информацией и определяющих меру ответственности за их нарушение.

2. Морально-этические нормы характеризуют нормы поведения обслуживающего персонала, которые традиционно сложились в данном обществе.

3. Административно-организационные меры связаны с подбором и подготовкой обслуживающего персонала, пропускным режимом, организацией хранения, учета и использования документации (информации), организацией контроля над персоналом, физическим ограничением на перемещение персонала в пределах данного предприятия (кодовые замки, блокировки и т. д.).

4. Программно-технические средства (ПТС) связаны с

-шифрованием информации;

-идентификацией (распознаванием и аутентификацией (проверкой подлинности) пользователей АСУ;

-контролем целостности информации;

-регистрацией и анализом событий в АСУ.

Первые операционные системы персональных компьютеров (MS-DOS, Windows версии до 3.1 включительно) не имели собственных программно-

технических средств защиты. Операционные системы Windows NT и Windows 2000 уже имеют программно-технические средства защиты.

Программно-технические средства защиты могут иметь 5 уровней.

Первый уровень. На этом уровне операционная система позволяет осуществлять защиту информации индивидуальному пользователю персонального компьютера на базе ее традиционных вспомогательных программ (утилит).

Второй уровень. АСУ имеют только системы идентификации и аутентификации пользователей. Эти системы ограничивают доступ к АСУ случайных и незаконных пользователей.

Третий уровень. АСУ обеспечивают шифрование данных (защита информации на дисках). Шифрование может осуществляться на уровне файла диска (архиватор типа arj) и на уровне всего диска (программа Discreet в пакете Norton Utilities).

Четвертый уровень. АСУ обеспечивают шифрование информации, передаваемой по каналам сети. Шифрование может быть канальным (всей информации, включая служебную) на базе системы OSI (Open System Interconnection) и конечным для шифрования только конфиденциальной информации (но не служебной).

Пятый уровень. АСУ производит аутентификацию как автора, так и самой передаваемой информации (текста) за счет использования кода или электронной цифровой подписи (отечественный стандарт ГОСТ 28 147-89).

### *Вопросы для самоконтроля*

*1. В чем отличие правовых от морально-этических норм построения надежных АСУ?*

*2. Могут ли административно-организационные меры компенсировать программно-технические средства построения надежных АСУ?*

*3. Перечислите уровни защиты информации и укажите сущность каждого уровня.*

# 10. ДИАГНОСТИКА И ПРОГРАММНАЯ НАДЕЖНОСТЬ АСУ, ПОСТРОЕННЫХ НА БАЗЕ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

При работе на персональном компьютере и использовании его либо в качестве управляющего устройства в АСУ, либо в качестве устройства обмена информацией в локальной вычислительной сети, либо, наконец, в качестве устройства временного (или постоянного) хранения секретной или конфиденциальной информации, необходимо соблюдать простые, но в ряде случаев достаточно эффективные, меры защиты информации или используемого программного обеспечения [5].

К таким мерам можно отнести:

1) временную блокировку монитора компьютера;

2) использование гибких магнитных дисков для длительного хранения информации;

3) резервное копирование информации;

4) очистку *Корзины* и меню *Документ*;

5) очистку дисков от удаленных файлов;

6) диагностику сохранности информации;

7) защиту информации от случайного изменения;

8) сокрытие файлов и папок;

9) защиту информации паролем.

1. При временном отлучении от компьютера и желании защитить свою информацию от нежелательных, но не очень сведущих в компьютерном деле посетителей, возможно произвести временную блокировку монитора компьютера за счет перехода в полноэкранный режим DOS. В этом режиме весь экран монитора становится темным с несколькими ничего не значащими для неопытного человека символами.

Для запуска режима DOS необходимо открыть меню **Пуск**, выбрать **Программы**, в открывшемся окне нажать **Сеанс MS DOS**. Весь экран монитора станет темным.

Для возврата из режима DOS необходимо набрать **EXIT** (**exit**) и нажать клавишу **Enter**.

Если **Сеанс MS DOS** открывается в небольшом окне поверх остальных окон, то необходимо нажать комбинацию клавиш **Alt+пробел** для вызова меню DOS, выбрать в нем команду **Развернуть** и повторить запуск режима DOS.

2. Использование гибких магнитных дисков для длительного хранения информации позволяет секретную или конфиденциальную информацию всегда хранить при себе. Для этого после завершения работы на компьютере необходимо скопировать информацию на гибкий магнитный диск с обязательным удалением из компьютера скопированной информации.

Копирование файла на гибкий диск:

-установить дискету в дисковод А;

-щелкнуть правой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **ПРОВОДНИК**;

-щелкнуть дважды левой клавишей мыши по искомой папке;

-щелкнуть правой клавишей мыши по копируемому файлу;

-щелкнуть левой клавишей мыши по пункту **ФАЙЛ**;

-щелкнуть левой клавишей мыши по пункту **КОПИРОВАТЬ**;

-щелкнуть левой клавишей мыши по пункту **ДИСК А**;

-щелкнуть правой клавишей мыши по свободному месту окна;

-щелкнуть левой клавишей мыши по пункту **ВСТАВИТЬ**.

Удаление файла:

-щелкнуть правой клавишей мыши по значку **МОЙ КОМПЬЮТЕР**;

-щелкнуть левой клавишей мыши по пункту **ПРОВОДНИК**;

-щелкнуть левой клавишей мыши по искомому диску в окне **Все папки**;

-щелкнуть дважды левой клавишей мыши по папке, в которой находится искомый файл;

-щелкнуть правой клавишей мыши по файлу, который надо удалить;

-щелкнуть левой клавишей мыши по пункту **УДАЛИТЬ**;

-ответить на вопрос компьютера.

3. Резервное копирование информации производится в тех случаях, когда имеется вероятность преднамеренного или случайного удаления программного обеспечения АСУ или разработанного файла, попадания в компьютер вируса или полного сбоя системы.

При установке программного обеспечения в этом случае необходимо создавать аварийный или системный диск. На этом диске должна находиться информация, достаточная операционной системе для запуска компьютера с диска А, а также некоторая информация о конфигурации компьютера. Этот диск следует хранить в безопасном месте.

Системный диск не может восстановить файлы данных, которые создаются при помощи различных приложений- текстовых процессоров, приложений электронных таблиц, графических редакторов, а также информации, полученной из внешних источников.

Существуют специальные программы резервного копирования, позволяющие быстро скопировать информацию, находящуюся на жестком диске компьютера на гибкие диски. Из этих программ широко используются Norton Backup и Fast Back Plus.

4. В соответствии со стандартными установками Windows удаленные файлы фактически сохраняются в папке *Корзина* вплоть до ее очистки. Это связано в ряде случаев с необходимостью восстановления случайно удаленных файлов. Поэтому в папке *Корзина* “удаленные” файлы можно не только просмотреть, но и восстановить. По этой причине корзину необходимо периодически очищать от скопившихся там “удаленных” файлов, которые могут представлять интерес для определенного круга лиц. Та же проблема стоит и в связи с удалением файлов из меню *Документы*.

Удаление файла из корзины:

-щелкнуть дважды левой клавишей мыши по значку **КОРЗИНА**;

-щелкнуть левой клавишей мыши по файлу, который надо удалить;

-щелкнуть левой клавишей мыши в строке меню по пункту **ФАЙЛ**;

-щелкнуть левой клавишей мыши по пункту **УДАЛИТЬ**;

-ответить на вопрос компьютера.

Вместо периодической очистки корзины возможно вообще отказаться от услуг корзины, произведя соответствующую настройку корзины.

Настройка *Корзины*:

-щелкнуть правой клавишей мыши по знаку **КОРЗИНА**;

-щелкнуть левой клавишей мыши по пункту **СВОЙСТВА**;

-щелкнуть левой клавишей мыши по вкладке **ГЛОБАЛЬНЫЕ**;

-установить переключатель на пункт **ЕДИНЫЕ ПАРАМЕТРЫ ДЛЯ ВСЕХ ДИСКОВ**;

-установить движок **МАКСИМАЛЬНЫЙ ОБЪЕМ КОРЗИНЫ** на 10%;

-установить флажок на пункте **ЗАПРАШИВАТЬ ПОДТВЕРЖДЕНИЕ НА УДАЛЕНИЕ**;

-щелкнуть левой клавишей мыши по кнопке **ОК**.

Если необходимо отказаться от услуг корзины, то после пункта *Единые параметры...*

-установить переключатель на пункт **УНИЧТОЖАТЬ ФАЙЛЫ СРАЗУ ПОСЛЕ УДАЛЕНИЯ, НЕ ПОМЕЩАЯ В КОРЗИНУ**;

-щелкнуть левой клавишей мыши по кнопке **ОК**.

Уничтожение удаленных файлов из меню *Документы*:

-щелкнуть левой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **НАСТРОЙКА**;

-щелкнуть клавишей мыши по пункту **ПАНЕЛЬ ЗАДАЧ**;

-в окне *Свойства: панель задач* щелкнуть левой клавишей по вкладке **НАСТРОЙКА МЕНЮ**;

-щелкнуть левой клавишей мыши по кнопке **ОЧИСТИТЬ**;

-щелкнуть левой клавишей мыши по кнопке **ОК**.

При этом необходим помнить, что после выполнения вышеуказанной операции в меню *Документы* уничтожаются все файлы.

5. В дисках, которые используются для хранения информации, применяются магнитные материалы. Информация хранится в отдельных намагниченных областях диска. Эти области диска называются секторами. Несколько секторов объединяются в кластеры. Секторы и кластеры образуют дорожки диска. Информация о размере и месте расположения файла на диске заносится в дорожки каталогов. Информация одного файла не обязательно будет располагаться в смежных секторах. Она может находится в любом месте диска. Когда файл, записанный на диск, удаляется, данные этого файла остаются на диске. В этом случае удаляется лишь информация о файле из каталога. После удаления файла сектора, в которые он был записан, становятся доступными для вновь создающихся файлов, так как компьютер воспринимает их как свободные. Данные вновь создаваемого файла записываются “поверх” данных уничтоженного файла без дополнительной операции стирания старой информации. Промежуток времени между уничтожением старого файла и вновь создаваемого, данные которого могут быть записаны в сектора удаленного файла, может быть использован посторонними лицами для восстановления уничтоженного файла при помощи специальных программ-утилит, например, Norton Unerase [6].

Для окончательного уничтожения данных аннулированного файла во всех секторах, которые он занимал на диске, используются специальные программы-утилиты, которые заполняют эти сектора либо нулями, либо случайными числами, при этом производят эти операции по несколько раз подряд для обеспечения требуемой надежности. К таким утилитам относятся McAfee Office 2000, Norton Utilites 2000 и Quarterdeck Remove-It [6].

6. Диагностика сохранности информации состоит в контроле текущего использования (открывания) файлов с секретной или конфиденциальной информацией. Диагностика может быть осуществлена несколькими способами.

Диагностика с помощью приложения *Проводник*:

-щелкнуть правой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **ПРОВОДНИК**;

-щелкнуть дважды левой клавишей мыши по искомой папке;

-щелкнуть правой клавишей мыши по искомому файлу;

-щелкнуть левой клавишей мыши по пункту **СВОЙСТВА**;

-щелкнуть левой клавишей мыши по вкладке **ОБЩИЕ** окна *Свойства*.

В средней части окна *Свойства* приведены время и дата создания файла и время и дата последнего его открытия или изменения. Если открытие или изменение файла последний раз осуществлялось после времени и даты последней работы над ним автором, то это значит, что этот файл кто-то открывал.

Для осуществлении диагностики сохранности файла также возможен просмотр диалогового окна *Свойства*, щелкнув правой клавишей мыши по искомому файлу в списке, который отображается командами *Файл- открыть*.

Диагностику сохранности файлов необходимо производить перед их открытием. В противном случае в окне *Свойства* будут утрачены дата и время открытия файла поверяющим.

7. Защита файла от изменения в нем информации при случайных воздействиях осуществляется за счет задания атрибута *Только чтение* в окне *Свойства*.

Защита от изменения информации:

-щелкнуть правой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **ПРОВОДНИК**;

-щелкнуть дважды левой клавишей мыши по искомой папке;

-щелкнуть правой клавишей мыши по искомому файлу;

-щелкнуть левой клавишей мыши по пункту **СВОЙСТВА**;

-щелкнуть левой клавишей мыши по вкладке **ОБЩИЕ** окна *Свойства*;

-щелкнуть левой клавишей мыши по пункту **ТОЛЬКО ЧТЕНИЕ**;

-щелкнуть левой клавишей мыши по кнопке **ОК**.

При атрибуте *Только чтение* нельзя изменять содержимое файла и удалять его командой *DEL*.

8. Сокрытие файла или папки сводится к удалению их названий из списка файлов или папок каталога, но при сохранении самого файла. Это дает возможность в некоторой степени предохранить информацию от преднамеренного искажения или хищения.

Сокрытие файла или папки:

-щелкнуть правой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **ПРОВОДНИК**;

-щелкнуть дважды левой клавишей мыши по искомой папке;

-щелкнуть правой клавишей мыши по искомому файлу;

-щелкнуть левой клавишей мыши по пункту **СВОЙСТВА**;

-щелкнуть левой клавишей мыши по вкладке **ОБЩИЕ** окна *Свойства*;

-щелкнуть левой клавишей мыши по пункту **СКРЫТЫЙ**;

-щелкнуть левой клавишей мыши по кнопке **ОК**;

-щелкнуть левой клавишей мыши по меню **ВИД**;

-щелкнуть левой клавишей мыши по пункту **ПАРАМЕТРЫ**;

-щелкнуть левой клавишей мыши по вкладке **ПРОСМОТР**;

-щелкнуть левой клавишей мыши по пункту **НЕ ОТОБРАЖАТЬ ФАЙЛЫ СЛЕДУЮЩИХ ТИПОВ**;

-щелкнуть левой клавишей мыши по кнопке **ОК**.

Для отмены режима сокрытия информации в предыдущей последовательности команд вместо строки

-щелкнуть левой клавишей мыши по пункту **НЕ ОТОБРАЖАТЬ ФАЙЛЫ СЛЕДУЮЩИХ ТИПОВ**;

использовать строку

-щелкнуть левой клавишей мыши по пункту **ОТОБРАЖАТЬ ВСЕ ФАЙЛЫ.**

9. Защита информации паролем чаще всего сводится либо к обеспечению невозможности включения (блокировки) программы Windows, либо к устранению попыток изменить информацию файла.

Блокировка программы Windows:

-щелкнуть левой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **НАСТРОЙКА**;

-щелкнуть левой клавишей мыши по пункту **ПАНЕЛЬ УПРАВЛЕНИЯ**;

-щелкнуть дважды левой клавишей мыши по пункту **ПАРОЛИ**;

-щелкнуть левой клавишей мыши по вкладке **СМЕНА ПАРОЛЕЙ**;

-щелкнуть левой клавишей мыши по кнопке **СМЕНИТЬ ПАРОЛЬ**;

-установить указатель мыши в текстовое поле **НОВЫЙ ПАРОЛЬ**;

-щелкнуть левой клавишей мыши;

-набрать на клавиатуре пароль;

-установить указатель мыши в поле **ПОДТВЕРЖДЕНИЕ ПАРОЛЯ**;

-щелкнуть левой клавишей мыши;

-набрать на клавиатуре тот же пароль;

-щелкнуть левой клавишей мыши по кнопке **ОК** и **ЗАКРЫТЬ**.

Смена пароля блокировки программы Windows:

-щелкнуть левой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **НАСТРОЙКА**;

-щелкнуть левой клавишей мыши по пункту **ПАНЕЛЬ УПРАВЛЕНИЯ**;

-щелкнуть дважды левой клавишей мыши по пункту **ПАРОЛИ**;

-щелкнуть левой клавишей мыши по вкладке **СМЕНА ПАРОЛЕЙ**;

-щелкнуть левой клавишей мыши по кнопке **СМЕНИТЬ ПАРОЛЬ**;

-набрать на клавиатуре действующий пароль в поле **СТАРЫЙ ПАРОЛЬ**;

-установить указатель мыши в поле **НОВЫЙ ПАРОЛЬ**;

-щелкнуть левой клавишей мыши;

-набрать на клавиатуре новый пароль;

-установить указатель мыши в поле **ПОДТВЕРЖДЕНИЕ ПАРОЛЯ**;

-щелкнуть левой клавишей мыши;

-набрать на клавиатуре новый пароль;

-щелкнуть левой клавишей мыши по кнопке **ОК** и **ЗАКРЫТЬ**.

Отмена блокировки программы Windows:

-щелкнуть левой клавишей мыши по кнопке **ПУСК**;

-щелкнуть левой клавишей мыши по пункту **НАСТРОЙКА**;

-щелкнуть левой клавишей мыши по пункту **ПАНЕЛЬ УПРАВЛЕНИЯ**;

-щелкнуть дважды левой клавишей мыши по пункту **ПАРОЛИ**;

-щелкнуть левой клавишей мыши по вкладке **СМЕНА ПАРОЛЕЙ**;

-щелкнуть левой клавишей мыши по кнопке **СМЕНИТЬ ПАРОЛЬ**;

-установить указатель мыши в текстовое поле **СТАРЫЙ ПАРОЛЬ**;

-щелкнуть левой клавишей мыши по кнопке **ОК** и **ЗАКРЫТЬ**.

Устранение попыток изменения информации файла вводом пароля:

-щелкнуть левой клавишей мыши в строке меню по пункту **СЕРВИС**;

-щелкнуть левой клавишей мыши по пункту **УСТАНОВИТЬ ЗАЩИТУ**;

-ввести пароль в текстовом поле и нажать кнопку **ОК**;

-подтвердить пароль в текстовом поле и нажать кнопку **ОК.**

***Вопросы для самоконтроля***

*1. Какие из мер защиты информации производятся на базе программы Windows?*

*2. Возможно ли полностью и в каком случае удалить информацию из персонального компьютера?*

*3. Какой способ хранения информации является наиболее надежным?*

*4. В чем отличие устранения попыток изменения информации файла вводом пароля от защиты файла от изменения информации вводом ограничения* ***ТОЛЬКО ЧТЕНИЕ****?*

## 11. КЛАССИЧЕСКИЕ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Наиболее надежным способом защиты информации в АСУ является ее шифрование [5,6]. Шифрование применяется человечеством очень давно и многие ее методы за это время стали классическими. Шифровальные методы с одним секретным ключом называются симметричными криптосистемами.

В переводе с греческого языка crypts значит тайный, а logos-сообщение. От совместного использования этих двух слов получены следующие термины.

*Криптология*-наука о секретных (тайных) сообщениях.

*Криптосистема* обеспечивает работу АСУ с секретной или конфиденциальной информацией.

*Криптоанализ* характеризует раскрытие секретной или конфиденциальной информации.

*Криптография* представляет собой совокупность методов преобразования информации, направленных на ее защиту от искажения или разглашение.

*Криптостойкость* оценивает способность зашифрованной информации противостоять криптоанализу.

*Криптограммой* называется зашифрованный при помощи специальных приемов текст или документ.

Криптология базируется на шифровании, которое заключается в переводе исходного текста в отвлеченные от данного текста символы по заранее выбранному алгоритму.

Шифрование должно удовлетворять следующим трем требованиям:

1) надежности закрытия текста;

2) простоте процесса шифрования и расшифрования;

3) стойкости к случайным помехам.

Симметричные криптосистемы могут использовать один секретный ключ как на стороне передачи информации, так и на стороне приема информации.

Существуют следующие методы шифрования:

1) метод перестановок;

2) метод замены;

3) метод гаммирования.

Все три метода могут быть использованы как с ключами, так и без них. Чаще эти методы используют с одним секретным ключом и поэтому их называют криптосистемами с одним секретным ключом или симметричными криптосистемами [6].

## 11.1. Метод перестановок

При этом методе символы исходного текста переставляются по определенному правилу в пределах блока шифруемого текста. Это самый простой и самый древний метод шифрования.

В большинстве случаев перестановка производится на базе таблиц без ключа или с ключом.

**Пример 11.1.1.** Зашифровать текст без ключа. Задан исходный блок текста:

ВЫПЛАТИТЬ ИВАНОВУ СТО РУБЛЕЙ.

Составляется таблица с количеством строк и столбцов, соответствующим количеству букв исходного текста. Текст в таблице записывается начиная с первого столбца сверху вниз (табл. 11.1.1).

*Таблица 11.1.1*

| | | | | |
|---|---|---|---|---|
| В | Т | В | У | У |
| Ы | И | А | С | Б |
| П | Т | Н | Т | Л |
| Л | Ь | О | О | Е |
| А | И | В | Р | Й |

Зашифрованный текст из таблицы считывается по строкам слева направо, начиная с первой строки. Зашифрованный текст будет иметь следующий вид ВТВУУ ЫИАСБ ПТНТЛ ЛЬООЕ АИВРЙ.

**Пример 11.1.2.** Зашифровать текст с ключом. Задан исходный блок текста: ВЫПЛАТИТЬ ИВАНОВУ СТО РУБЛЕЙ.

В этом случае в табл. 11.1.1 добавляются две первые строки (табл.11.1.2). В первую строку помещается ключ в виде заранее выбранного слова (например, ВИЛКА), а во вторую строку помещают цифры, характеризующие порядок букв ключа в русском алфавите. Ключ (ключевое слово) является секретным и не подлежит разглашению.

Табл. 11.1.2 преобразуется путем перемещения столбцов. Столбцы располагаются в соответствии с указанными номерами букв ключа (табл. 11.1.3).

*Таблица 11.1.2*

| | | | | |
|---|---|---|---|---|
| В | И | Л | К | А |
| 2 | 3 | 5 | 4 | 1 |
| В | Т | В | У | У |
| Ы | И | А | С | Б |
| П | Т | Н | Т | Л |
| Л | Ь | О | О | Е |
| А | И | В | Р | Й |

*Таблица 11.1.3*

| А | В | И | К | Л |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| У | В | Т | У | В |
| Б | Ы | И | С | А |
| Л | П | Т | Т | Н |
| Е | Л | Ь | О | О |
| Й | А | И | Р | В |

Зашифрованный текст из таблицы (табл.11.1.3) считывается по строкам слева направо, начиная с третьей строки. Зашифрованный текст будет иметь следующий вид

УВТУВ БЫИСА ЛПТТН ЕЛЬОО ЙАИРВ.

Возможно производить повторное шифрование (цикл шифрования). Расшифрование текста производится в обратном порядке.

## 11.2. Метод замены

При этом методе шифрования символы исходного текста заменяются символами другого алфавита по заранее установленным правилам с применением ключа или без него (метод Гай Юлия Цезаря, 50 г до н.э.).

**Пример 11.2.1.** Зашифровать исходный текст без ключа, используя в качестве новых символов шифрования буквы русского алфавита.

Исходный текст

ВЫПЛАТИТЬ СТО РУБЛЕЙ.

В качестве символов шифрования используются буквы русского алфавита, смещенные относительно исходного алфавита на некоторую величину q, например q=3. В этом случае оба алфавита расположатся следующим образом

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 Ъ Э Ю Я

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 Ъ Э Ю Я **А Б В**

Зашифрованный текст примет вид

ЕЮТОГХЛХЭФХСУЦДОИМ.

**Пример 11.2.2.** Зашифровать исходный текст с ключом, используя в качестве новых символов шифрования буквы русского алфавита.

Исходный текст

ВЫПЛАТИТЬ СТО РУБЛЕЙ.

В качестве ключа выбрано ключевое слово

АРГУМЕНТ.

В таблицу сначала вписывается ключевое слово, а затем символы русского алфавита, пропуская буквы входящие в это ключевое слово (табл. 11.2.1).

*Таблица11.2.1*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| А | Р | Г | У | М | Е | Н | Т |
| Б | В | Д | Ж | З | И | Й | К |
| Л | О | П | С | Ф | Х | Ц | Ч |
| Ш | Щ | Ь | Ы | Ъ | Э | Ю | Я |

Для выполнения процесса шифрования в таблице находится очередная буква исходного текста и в шифровку записывается буква, расположенная ниже ее в том же столбце. Если буква исходного текста оказывается в нижней строке, тогда берется буква из верхней строки того же столбца. При этом в формировании зашифрованного текста участвуют и буквы ключевого слова.

Зашифрованный текст будет иметь вид

ОУЬШБКХКГ ЫКЩ ВЖЛШИЦ.

## 11.3. Метод гаммирования

Метод гаммирования базируется на операции логического сложения по модулю 2 (символ ⊕). Например, если складывать по модулю 2 два аргумента, представленные в двоичной системе счисления, то можно записать

0⊕0=0, 0⊕1=1, 1⊕0=1, 1⊕1=0.

При использовании этого метода кодовые комбинации, характеризующие буквы исходного текста, складываются по модулю 2 с псевдослучайными кодовыми комбинациями, генерируемыми компьютером.

**Пример 11.3.1.** Зашифровать исходный текст

ИДЕАЛ.

Компьютеры могут обрабатывать только информацию, представленную в числовой форме. При вводе исходного текста, вводимые буквы кодируются определенными числами (кодовыми комбинациями), а при выводе их на монитор или принтер по каждой кодовой комбинации строится изображение буквы. Соответствие между буквами исходного текста и их кодовыми комбинациями называется кодировкой символов. На импортных компьютерах кодировка производится в коде ASC11. В нашей стране создана модифицированная альтернативная кодировка - ГОСТ символов русского алфавита с кодовыми комбинациями в диапазоне от 128 до 239 (от А до Я). При методе гаммирования кодовые комбинации букв модифицированного альтернативного алфавита складываются с псевдослучайными кодовыми комбинациями, генерируемыми компьютером. Но для простоты понимания процесса шифрования методом гаммирования предположим, что буквы исходного текста в компьютере выражаются кодовыми комбинациями как это указано ниже

| А | Б | В | Г | Д | Е | Ж |
|---|---|---|---|---|---|---|
| 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |

| З | И | Й | К | Л... |
|---|---|---|---|---|
| 1000 | 1001 | 1010 | 1011 | 1100... |

Предположим, что компьютер генерирует псевдослучайную последовательность кодовых комбинаций вида (числа генерируются случайные по своему значению, но всегда в строго определенной последовательности)

0101, 0010, 0100, 0001, 0011, 0111, 0110 ...

Производится сложение по модулю 2 кодовых комбинаций исходного текста и кодовых комбинаций псевдослучайной последовательности

| И | Д | Е | А | Л |
|---|---|---|---|---|
| 0101 | 0010 | 0100 | 0001 | 0011 |
| 1001 | 0101 | 0110 | 0001 | 1100 |
| 1100 | 0111 | 0010 | 0000 | 1111 |

Зашифрованный текст примет вид

1100, 0111, 0010, 0000, 1111.

Расшифрование производится повторным сложением по модулю 2 кодовых комбинаций зашифрованного текста с кодовыми комбинациями псевдослучайной последовательности.

| И | Д | Е | А | Л |
|---|---|---|---|---|
| 0101 | 0010 | 0100 | 0001 | 0011 |
| 1100 | 0111 | 0010 | 0000 | 1111 |
| 1001 | 0101 | 0110 | 0001 | 1100. |

В данном методе шифрования кодовые комбинации псевдослучайной последовательности образуются из так называемой ключевой последовательности, где первая кодовая комбинация ключевой последовательности называется ключом (0101).

Псевдослучайная последовательность двоичных кодовых комбинаций формируется из ключевого потока путем последовательного формирования групп с добавлением нуля в старшем двоичном разряде каждой группы.

Предположим, ключевой поток имеет вид

1010011.

Тогда псевдослучайные кодовые комбинации, получаемые из ключевого потока, примут вид

**101**0011→0101; 1**010**011→0010; 10**100**11→0100; 101**001**1→0001;

1010**011**→0011; **1**0100**11**→0111; **10**1001**1**→0110.

После генерации кодовой комбинации 0110 последовательность кодовых комбинаций повторяется. Чем длиннее ключевой поток, тем большая криптостойкость шифрования.

***Вопросы для самоконтроля***

1. *Какую роль выполняет ключ при шифровании информации?*
2. *Для чего применяется повторное шифрование одной и той же информации?*
3. *В чем отличие кодировки в коде ASC11 от кодировки в модифицированном альтернативном коде ГОСТ?*

## 12. СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ

При создании современных криптосистем использовались одновременно все три метода шифрования с ключами и многократными циклами повторения процесса шифрования одного и того же исходного текста [6].

### 12.1. Американский стандарт шифрования данных DES

*DES-(*Data Encryption Standard) опубликован в 1977 году и предназначен для защиты несекретной информации в государственных и коммерческих организациях (банкоматах). Разработчик *DES* фирма IBM. Первоначально эта криптосистема использовалась для внутренних целей фирмы под названием "Люцифер".

Характеристики DES.

1. Обработка (шифрование) исходного текста производится блоками по 64 бит каждый.

2. Шифрование сочетает перестановку, замену и гаммирование в определенной последовательности 16- кратными повторяющимися циклами.

3. Ключ имеет разрядность 56 бит. Если использовать компьютер с производительностью 1 миллион анализируемых вариантов в секунду, то потребуется 2285 лет для опробования всех возможных ключей, которые можно составить из кода в 56 бит ($2^{56}$).

### 12.2. Алгоритм шифрования данных IDEA

*IDEA*-(International Data Encryption Algorithm)-опубликован в 1990 году. Это дальнейшая разработка *DES*, но в ней удлинен объем ключа до 128 бит. При $2^{128}$ потребуется не 2285, а $10^{25}$ лет (возраст вселенной $10^{10}$ лет) для перебора всех возможных комбинаций ключей. Используется IDEA только с персональными компьютерами, имеющими процессор не ниже 486.

#### *Вопросы для самоконтроля*

*1. В чем состоит трудность раскрытия зашифрованной информации, учитывая современный уровень развития компьютеров?*

3. *В чем отличие стандарта шифрования данных DES от его дальнейшей модернизации IDEA.*

## 13. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

В математике функция, не имеющая обратного преобразования или имеющая бесконечное множество обратных преобразований, называется *однонаправленной*.

**Пример 13.1.** Дана однонаправленная функция вида

$$N = P \cdot Q .$$

Если известны $P$ и $Q$, то легко вычислить $N$. Но если известно $N$, но неизвестны $P$ и $Q$, то найти истинные (заранее заданные) значения $P$ и $Q$ по известной величине $N$ невозможно.

Если, в свою очередь, $P$ и $Q$ входят в другие математические зависимости, функционально связанные с однонаправленной функцией, по которым возможно оценить их истинные значения, то возможно подобрать $P$ и

$Q$ из условия тождества однонаправленной функции и данной математической зависимости.

**Пример 13.2.** Дана однонаправленная функция

$$N = P \cdot Q$$

и математическое выражение вида

$$P + Q^2 = A.$$

Официально известно, что $N$=12 и $A$=10.

Найти истинные значения $P$ и $Q$.

Возможны следующие варианты значений $P$ и $Q$ (используются только целые числа):

1) $P$=1; $Q$=12; тогда $1+12^2=1+144=145$;

2) $P$=2; $Q$=6; тогда $2+6^2=2+36=38$;

3) $P$=3; $Q$=4; тогда $3+4^2=3+16=19$;

4) $P$=4 $Q$=3; тогда $4+3^2=4+9=13$;

5) $P$=6 $Q$=2; тогда $6+2^2=6+4=10$;

6) $P$=12 $Q$=1; тогда $12+1^2=12+1=13$.

Истинные значения $P$ и $Q$: $P$=6 и $Q$=2.

При очень большом значении $N$ (например, $N=2^{664}$) перебор значений $P$ и $Q$ становится практически неразрешимой задачей даже для быстродействующих ЭВМ.

В криптосистемах в качестве однонаправленной функции чаще используется дискретный логарифм вида

$$Y = A^X \bmod N,$$

где mod N–выбранная система счисления (модуль).

Дискретный логарифм при известных $Y$, $X$ и $N$ имеет бесконечное множество значений $A$.

Но решение дискретного логарифма может быть найдено если параметры $X$ и $N$ связать определенной зависимостью, которую можно условно назвать ключом. При этом, как правило, используются две зависимости - два ключа:

открытый ключ $K_0$ (не секретный), которым зашифровывается информация отправителя, и закрытый ключ $K_3$ (секретный), которым расшифровывается информация получателем.

Два числа *A* и *B* называются *сравнимыми по модулю N*, если их разность (*A*-*B*) делится на *N* без остатка.

Сравнение чисел *A* и *B* по модулю *N* справедливо тогда и только тогда, если

$$\frac{A-B}{N}=k\ ,$$

где *k*–целое положительное число.

Сравнение по модулю N выражается математически как

$$A \equiv B\ (mod\ N)$$

или

$$A\ (mod\ N) = B.$$

Число *N* называют *модулем сравнения*.

Число *B* называют *вычетом* числа *A* по модулю *N*.

Набор целых чисел B, лежащих в диапазоне от 0 до (*N*-1), называется *полным набором вычетов по модулю N*. Таким образом, для любого целого числа *A* его вычет по модулю *N* есть также некоторое целое число, численное значение которого находится в интервале от 0 до (*N*-1) и определяется выражением вида

$$B = A - k \cdot N.$$

Нахождение вычета *B* числа *A* по модулю *N* называется *приведением числа A по модулю N* или просто *приведением по модулю*.

Число *B* можно представить как *остаток* от деления числа *A* на модуль *N*.

Если *A*>*N*, то при делении числа *A* на модуль *N* в общем случае частное будет состоять из целого числа *k* и остатка *B*.

**Пример 13.3**. Произвести приведение по модулю 11 (*N*) числа 37 (*A*).

При делении числа 37 (число $A$) на число 11 (модуль $N$) получится частное 3 (целое число $k$) и остаток 4 (вычет $B$). Сравнение по модулю $N$ чисел $A$ и $B$ в этом случае можно записать как

$$37 \ (\text{mod } 11)=4$$

или

$$37 \equiv 4 \ (\text{mod } 11).$$

Справедливость полученного результата можно проверить по формуле

$$B=A-k\cdot N=4=37-3\cdot 11=4.$$

Если $A<N$, то при делении числа $A$ на модуль $N$ частное будет состоять из $k=0$ и остатка $B$, равного самому числу $A$.

**Пример 13.4.** Произвести приведение по модулю 7 *(N)* числа 2 ($A$).

При делении числа 2 (число $A$) на число 7 (модуль $N$) получится частное 0 (целое число $k$) и остаток 2 (вычет $B$). Сравнение по модулю $N$ чисел $A$ и $B$ в этом случае можно записать как

$$2 \ (mod \ 7)=2$$

или

$$2 \equiv 2 \ (mod \ 7).$$

Справедливость полученного результата можно проверить по формуле

$$B=A-k\cdot N=2=2-0\cdot 7=2.$$

Целые числа по модулю N с использованием операций сложения и умножения аналогичны свойствам обычных равенств.

**Пример 13.5.** Произвести операцию приведения по модулю 25 ($N$) числа $9^2$ ($A$). В этом случае можно записать

$$A \ (mod \ N)=B$$

или

$$81 \ (mod \ 25)=6.$$

Действительно,

$$B=A-k\cdot N=81-3\cdot 25=6.$$

В криптосистемах особое место занимают дискретные логарифмы с обратными величинами.

В арифметике действительных чисел обратную величину обозначают как

$$A^{-1} = \frac{1}{A}.$$

Выражение математической операции приведения обратного числа $A^{-1}$ по модулю N в этом случае примет вид

$$A^{-1} \equiv B \ (mod\ N)$$

или

$$\frac{1}{A} \equiv B(\mathrm{mod}\, N)$$

или

$$B \cdot A \ (mod\ N) = 1.$$

В криптосистемах чаще задача сводится к нахождению $B$ из выражения

$$A^{-1} \equiv B \ (mod\ N),$$

которое эквивалентно нахождению таких зависимостей $B$ и $k$, что

$$\frac{A \cdot B - 1}{N} = k.$$

Не всегда существует решение операции приведения обратного числа $A$ по модулю $N$. Решение существует если $A$ и $N$ взаимно простые числа, т.е. эти два числа имеют наибольший общий делитель (НОД) равный лишь единице

$$\text{НОД}\ (A, N) = 1,$$

а значение B заключено в пределах от 1 до (N-1).

**Пример 13.6**. Обратная величина для чисел $A$=5 и $N$=19 имеет решение $B$=4.

Действительно, подставив в выражение

$$B \cdot A \ (mod\ N) = 1,$$

значения $A$=5 и $N$=19 получим

$$(4 \cdot 5)\ (mod\ N) = 20\ (mod\ 19) = 1,$$

так как

$$B = \frac{N \cdot k + 1}{A} = \frac{19 \cdot 1 + 1}{5} = 4.$$

Обратная же величина для чисел $A$=2 и $N$=14 не имеет решения, так как

НОД ($A$, $N$)=2≠1

Действительно, при любом положительном целом числе $k$, величина B будет дробным числом, что недопустимо.

Существуют три способа нахождения обратной величины.

1. Проверка всех значений величины B в диапазоне от 1 до (n-1), пока не будет найдено искомое значение (способ перебора значений B).

2. Выполнение операции приведения обратного числа $A$ по модулю $N$ с участием функции Эйлера.

3. Выполнение операции приведения обратного числа $A$ по модулю $N$ с использованием расширенного алгоритма Евклида.

**Пример 13.7**. Найти значение $B$ в выражении

$$B=A^{-1} \ (mod\ N)$$

или

$$B \cdot A \equiv 1 \ (mod\ N)$$

при A=5 и N=7.

Используется первый способ.

Для данного примера наибольший общий делитель равен единице

НОД (A, $N$)=1

и значение B лежит в пределах от 1 до ($N$-1)=(7-1)=6.

Все возможные варианты решений сведены в табл. 13.1.

*Таблица 13.1*

| B | B·A | $B \cdot A \pmod N = 1$ |
|---|---|---|
| 1 | 5 | $1 \cdot 5 \pmod 7 = 5$ |
| 2 | 10 | $2 \cdot 5 \pmod 7 = 3$ |
| 3 | 15 | $3 \cdot 5 \pmod 7 = 1$ |
| 4 | 20 | $4 \cdot 5 \pmod 7 = 6$ |
| 5 | 25 | $5 \cdot 5 \pmod 7 = 4$ |
| 6 | 30 | $6 \cdot 5 \pmod 7 = 2$ |

Значение $B = 3$ так как при этом значении

$$B \cdot A \pmod N = 3 \cdot 5 = (\mathrm{mod}\ 7) = 1.$$

Справедливость полученного результата можно проверить по формуле

$$B = \frac{N \cdot k + 1}{A} = \frac{7 \cdot 2 + 1}{5} = 3.$$

***Вопросы для самоконтроля***

*1. В чем состоит особенность однонаправленной функции?*

*2. В чем состоит трудность нахождения решения дискретного логарифма?*

*3. Что представляет собой величина B в дискретном логарифме?*

***Задачи для самоконтроля***

*1. Найти значение B при A=243 и N=16. Ответ: B=3.*

*2. Найти значение B в выражении*

$$B \cdot A \pmod N = 1$$

*при A=5 и N=8. Ответ: B=13.*

# 14. АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Характерной особенностью асимметричных криптосистем является наличие двух ключей и использование для шифрования информации однонаправленных функций [6].

В этих системах один ключ используется для шифрования информации отправителем и является открытым ключом (несекретным), а второй ключ предназначен для расшифровки информации получателем и является закрытым (секретным). Открытый ключ рассылается всем пользователям компьютерной сети по открытым каналам связи. Закрытый ключ должен находиться в защищенном месте и не подлежит разглашению.

В этом случае программно-логическая модель криптосистемы примет вид, как указано на рис. 14.1.

На стороне получателя генерируются модуль *N*, открытые и закрытые ключи *(N, $K_O$ и $K_З$)*. Открытые ключи рассылаются всем пользователям системы. Закрытый ключ остается только у получателя. Отправитель зашифровывает при помощи открытого ключа символы исходного текста $K_O(M_j)$ и в виде криптограммы $C_i$ посылает получателю. Получатель при помощи закрытого ключа расшифровывает полученную криптограмму $K_З(C_i)$. В результате этого преобразования на стороне получателя образуются символы передаваемого текста Mj.

Работа асимметричной криптосистемы состоит из следующих этапов.

1. Генерация ключей.

В генераторе ключей задаются значения *P* и *Q* и вычисляется модуль

$$N=P\cdot Q.$$

Определяется количество положительных целых чисел в интервале от 1 до (N-1) по функции Эйлера

$$\varphi(N)=(P-1)\cdot(Q-1),$$

которые взаимно простые с модулем N.

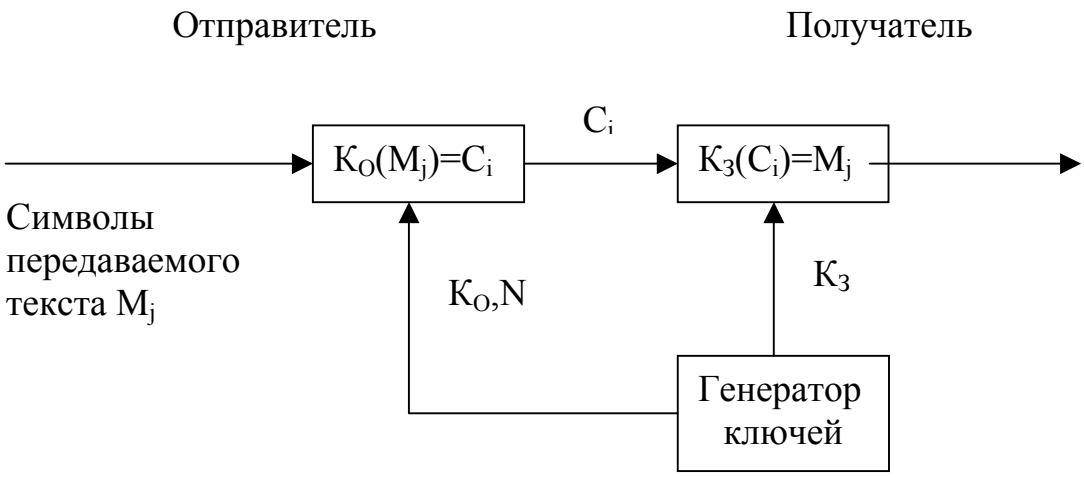


Рис.14.1. Программно-логическая модель асимметричной криптосистемы

Выбирается открытый ключ из условий

$$1<K_O\le\varphi(N)$$

и

$$НОД\ (K_O,\ \varphi(N))=1.$$

С использованием открытого ключа вычисляется закрытый ключ по формуле

$$K_3 \equiv K_O^{-1}(\bmod\ \varphi(N))\ .$$

2. Шифрование информации на стороне отправителя.

Получив от получателя значения модуля N и открытого ключа $K_O$ происходит шифрование символов исходного текста

$$C_j = M_j^{K_0}(\bmod N),$$

где j–признак очередного символа исходного текста.

3. Расшифрование информации на стороне получателя.

Используя закрытый ключ, происходит расшифровывание полученной криптограммы по формуле

$$M_j = C_j^{K_3} (\bmod N).$$

Работу асимметричной криптосистемы можно пояснить на следующем примере. Для облегчения расчетов используются малые числа.

**Пример 14.1**. Предположим, что необходимо передать сообщение вида

*DABC.*

Действия получателя информации.

1. Выбираются значения *P* и *Q*, например

$$P=2 \text{ и } Q=11.$$

2. Вычисляется модуль *N*

$$N=P \cdot Q=2 \cdot 11=22.$$

3. Вычисляется функция Эйлера

$$\varphi(N)=(P-1) \cdot (Q-1)=1 \cdot 10=10.$$

4. Выбирается открытый ключ из условия

$$1<K_0<\varphi(N) \text{ и НОД } (K_O, \varphi(N)).$$

Предположим $K_0=7$.

5. Вычисляется закрытый (секретный) ключ способом перебора (табл. 14.1).

*Таблица 14.1*

| $K_З$ | $K_З \cdot K_O$ | $K_З \cdot K_O \pmod{\varphi(N)}=1$ |
|---|---|---|
| 1 | 7 | $1 \cdot 7 \pmod{10}=7$ |
| 2 | 14 | $2 \cdot 7 \pmod{10}=4$ |
| 3 | 21 | $3 \cdot 7 \pmod{10}=1$ |

Действительно,

$$K_З \equiv K_0^{-1} [mod\ \varphi(N)]=7^{-1} mod\ 10=3.$$

6. Пересылаются отправителю значения

$$N=22 \text{ и } K_0=7.$$

Действия отправителя информации.

1. Предположим, что все символы пересылаемого текста имеют открытые и всем известные номера. Например *A*=2, *B*=3, *C*=4, *D*=5...

2. Производится шифрование пересылаемого текста $M_j$ открытым ключом по формуле

$$C_j = M_j (\bmod N).$$

Используя значения $K_O$, N=22 и $M_j$ находятся $C_j$

$$C_D = D^{K_0} (\bmod N) = 5^7 (\bmod 22) = 78125 (\bmod 22) = 3,$$

$$C_A = A^{K_0} (\bmod N) = 2^7 (\bmod 22) = 128 (\bmod 22) = 18,$$

$$C_B = B^{K_0} (\bmod N) = 3^7 (\bmod 22) = 2187 (\bmod 22) = 9,$$

$$C_C = C^{K_0} (\bmod N) = 4^7 (\bmod 22) = 16384 (\bmod 22) = 16.$$

Символы передаваемого текста отправляется получателю в виде криптограммы

3 18 9 16.

Действия получателя информации.

1. Расшифровывается полученная криптограмма закрытым (секретным) ключом по формуле

$$M_j = C_{M_j}^{K_3} (\bmod N).$$

Используя значения $K_З$, N=22 и $C_j$ находятся $M_j$

$$D = C_D^{K_3} (\bmod N) = 3^3 (\bmod 22) = 27 (\bmod 22) = 5,$$

$$A = C_A^{K_3} (\bmod N) = 18^3 (\bmod 22) = 5832 (\bmod 22) = 2,$$

$$B = C_B^{K_3} (\bmod N) = 9^3 (\bmod 22) = 729 (\bmod 22) = 3,$$

$$C = C_C^{K_3} (\bmod N) = 16^3 (\bmod 22) = 4096 (\bmod 22) = 4.$$

2. Полученные номера символов переводятся в сами символы передаваемой информации

$$5 \Rightarrow D,\ 2 \Rightarrow A,\ 3 \Rightarrow B,\ 4 \Rightarrow C.$$

***Вопросы для самоконтроля***

*1. Может ли отправитель информации генерировать и пересылать секретный ключ?*

*2. Что характеризует собой функция Эйлера?*

*3. Для всех ли значений положительных целых чисел существуют решения дискретного логарифма?*

## 15. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

*Идентификация* (от латинского слова identificare-отождествление) это совпадение каких либо двух событий, например, отождествление автора с разработанным им текстом.

*Аутентификация* (от латинского слова aunyentikos-подтверждение) это подтверждение подлинности чего-либо, например, подлинности имени автора текста.

При эксплуатации локальных вычислительных сетей, входящих в АСУ, должны выполняться две основные задачи [5,6].

1. Допуск пользователя сети к ее ресурсам.

Прежде чем получить доступ к ресурсам компьютерной сети пользователь должен:

-сообщить системе свое имя (число, символ, алгоритм), определяющий пользователя- идентификатор;

-подтвердить подлинность лица, идентификатор которого был объявлен-аутентификатор (электронная подпись, пароль).

2. Обеспечение надежного обмена информацией между пользователями компьютерной системы.

Для решения этой задачи должны быть выполнены следующие условия.

Получатель информации должен быть уверен:

-в подлинности отправителя;

-в подлинности полученной информации.

Отправитель информации должен быть уверен:

-в доставке информации получателю;

-в отсутствии искажений в доставленной получателю информации.

Для решения всех этих задач используется цифровая подпись (ЦП) по аналогии с рукописной подписью автора на документе, отпечатанном на бумаге.

Цифровая подпись должна содержать следующую информацию.

1. Дату подписи.
2. Срок окончания действия подписи.
3. Информацию об авторе (фамилию, имя, отчество, должность, наименование учреждения...).
4. Имя открытого ключа для расшифровки подписи.
5. Собственно цифровую подпись (СЦП).

Для постановки цифровой подписи используется закрытый (секретный) ключ $K_З$ и при расшифровке цифровой подписи используется открытый (несекретный) ключ $K_0$.

При формировании цифровой подписи компьютер отправителя информации ($A$) вычисляет однонаправленную *хэш-функцию* $m_A = h(M)$ подписываемого блока текста М (рис. 15.1). Хэш-функция $m_A = h(M)$ представляет собой один короткий блок информации (код), характеризующий весь блок текста М в целом в сжатой форме. Затем этот блок информации подлежит шифрованию закрытым (секретным) ключом ($K_З$) отправителя

$$S = m^{K_З} \bmod N$$

и результат шифрования $S$ вместе с текстом $M$ пересылается получателю ($B$).

Компьютер на стороне получателя информации снова вычисляет хэш-функцию $m_B = h(M)$ полученного блока текста $M$ и при помощи открытого ключа ($K_0$) расшифровывает полученную зашифрованную хэш-функцию $S$. Далее происходит сравнение двух хэш-функций: вновь полученной на стороне получателя $m_B$ на базе полученного текста $M$ и хэш-функции, расшифрованной открытым ключом $m_A$. Это позволяет проверить соответствует ли полученная

от отправителя цифровая подпись вычисленному значению $m_B$ блока информации *M*.

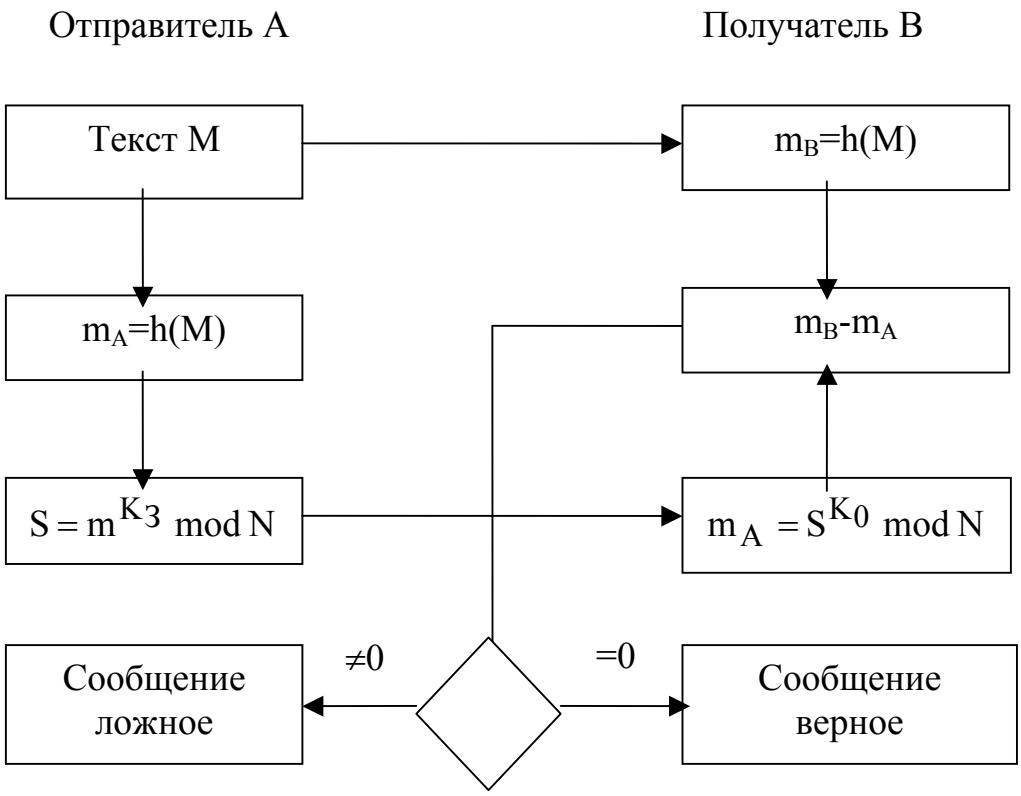


Рис.15.1. Схема проверки подлинности подписи отправителя

### *Вопросы для самопроверки*

*1. В чем отличие цифровой подписи от обычной подписи на бумаге?*

*2. Какую роль выполняет хэш-функция?*

*3. Производится ли шифрование текста при использовании цифровой подписи?*

# 16. ОРГАНИЗАЦИЯ СИСТЕМЫ КЛЮЧЕЙ

При использовании симметричных и асимметричных криптосистем применяются открытые и закрытые ключи для шифрования и расшифрования пересылаемой информации.

Основная задача организации системы ключей состоит в обеспечении надежной защиты ключевой информации от злоумышленников [5,6].

Комплекс мер защиты ключевой информации представляет собой совокупность программных и аппаратных средств:

-генерацию ключей;

-хранение ключей;

-распределение ключей.

## 16.1. Генерация ключей

Для обеспечения надежности ключевой информации необходимо:

-иметь достаточную длину (разрядность кодовой комбинации) и случайную зависимость расположения битов ключевого потока, из которого формируются ключи (гаммирование, выбор $P$ и $Q$ в случае использования дискретного логарифма);

-осуществлять регулярную модификацию ключей с целью исключения раскрытия ключа на базе статистических данных.

Для формирования ключей используются как аппаратные (генераторы псевдослучайных чисел, собранные на отдельной плате), так и программные средства.

Сущность создания ключа состоит в генерации (выборе) простых чисел P и Q (в случае использования дискретного логарифма в качестве однонаправленной функции) являющимися сомножителями модуля (основанием выбранной системы счисления)

$$N=P\cdot Q.$$

Наличие сомножителей P и Q позволяет вычислить функцию Эйлера

$$\varphi(N)=(P-1)\cdot(Q-1),$$

а затем определить (задать) значение закрытого ключа по алгоритму Евклида

$$K_З = K_0^{-1} \bmod N .$$

Следовательно, значения *P* и *Q* являются исходными, а знание этих значений позволяет найти закрытый ключ. Поэтому генерации чисел, определяющих значения *P* и *Q*, придается первостепенное значение. После расчета закрытого ключа значения *P* и *Q*, как правило, уничтожаются.

Для повышения криптостойкости ключей значения *P* и *Q* выбираются из достаточно больших по объему двоичных чисел и с увеличением производительности компьютеров (исключение криптоанализа) постоянно увеличиваются (табл. 16.1) [1].

Например, в 1994 году ключ с объемом в 129 десятичных разрядов раскрыли 1600 одновременно работающих в сети компьютеров за 8 месяцев (240 дней).

Количество бит ключей для асимметричных криптосистем

*Таблица 16.1*

| Год | Отдельные пользователи | Корпорации | Государственные организации |
|---|---|---|---|
| 1995 | 768 | 1280 | 1536 |
| 2000 | 1024 | 1280 | 1536 |
| 2005 | 1280 | 1536 | 2048 |
| 2010 | 1280 | 1536 | 2048 |

В настоящее время в системе *RSA* созданы специальные аппаратные средства на базе сверхбольших интегральных схем (СБМС), в основу работы которых положены математические процессоры. Эти сверхмощные процессоры позволяют возводить большие числа в очень большие степени и тем самым создавать криптостойкие ключи.

### 16.2. Хранение ключей

Для защиты и хранения ключей вводится иерархия ключей.

1. Ключ шифрования данных (рабочий сеансный ключ)- КД.

2. Ключ шифрования ключей (пересылка ключей, хранение ключей)- КК.

3. Мастер-ключ (главный ключ) для шифрования ключа шифрования ключей (КК) при их хранении.

Ключи шифрования данных (КД) постоянно пересылаются между субъектами компьютерной сети или находятся внутри компьютера. Они часто модернизируются.

Ключи шифрования ключей (КК) не используются для шифрования данных, а только для шифрования ключей шифрования данных (КД) и тоже постоянно находятся в компьютере каждого субъекта компьютерной сети.

Мастер-ключ фиксируется на длительное время (до месяца). Для каждого компьютера имеется свой один мастер-ключ, который помещается в защищенный от считывания и записи, а так же от механических воздействий, блок в виде сверхбольшой интегральной схемы в физически защищенное место. Мастер-ключ передается только при персональном общении субъектов компьютерной сети.

Носителем ключевой информации (КД и КК) могут быть магнитные диски или пластиковые карты.

### 16.3. Распределение ключей

Под распределением ключей понимается либо снабжение текущими ключами абонентов корпоративной локальной сети, либо обмен ключами между получателями и отправителями этой сети.

Распределение ключей может реализовываться двумя способами:

1) использование центрального сервера (компьютера) данной локальной сети для централизованной генерации и рассылки текущих ключей;

2) прямым обменом ключами шифрования данных (КД) между пользователями компьютерной сети.

В обоих случаях должна быть обеспечена подлинность сеанса связи (идентификация и аутентификация). Как правило в этом случае используется механизм запроса и ответа.

Например, пользователь А для аутентификации включает в посылаемый запрос для пользователя В непредсказуемый элемент, например большое случайное число, заранее пользователю В неизвестное. В ответ пользователь В должен произвести над этим числом по предварительной договоренности с пользователем А некоторую математическую операцию, например вычесть корень из этого числа, и результат переслать пользователю А. По результату пользователь А судит о подлинности партнера в компьютерной сети.

### *Вопросы для самоконтроля*

1. *Какую цель преследует организация системы ключей?*
2. *Поясните иерархию ключей.*
3. *В чем отличие идентификации от аутентификации?*

## 17. КОМПЬЮТЕРНЫЕ ВИРУСЫ

Угрозу нарушению целостности информации (ее искажению, удалению и подмене), а, следовательно, и работоспособности АСУ, представляют компьютерные вирусы [5].

*Компьютерный вирус* – это программы или макросы, выполняющие некоторые, нежелательные для пользователя действия, препятствующие нормальной работе компьютера, разрушающие файловую структуру дисков и хранимую в компьютере информацию.

Пути проникновения компьютерных вирусов – через гибкие и CD- диски, а также сети (включая Интернет). Компьютерные вирусы могут распространяться крайне быстро, засоряя память и разрушая программы и данные.

По тому действию, которое выполняют компьютерные вирусы, существуют следующие их разновидности:

- Вирусы-разрушители. Повреждают и удаляют файлы при запуске, зараженных вирусом программ. Увеличивают размер и содержимое файлов.
- Вирусы самовоспроизводящиеся. Самопроизвольно размножаются и распространяются, постоянно инфицируя другие файлы.
- Вирусы-похитители. Похищают имена пользовательских программ и пароли доступа к различного рода службам. Перехватывают данные для дальнейшего заражения и размножения программ.
- Вирусы-управляющие. Захватывают управление персональным компьютером, вызывают перезагрузку программ и самого компьютера.
- Макровирусы. Загружаются вместе с макросами, повреждая и захватывая данные.
- Вирусы-помехи. Выводят звуковые и текстовые сообщения, переключают окна и т.д.
- Вирусы-апплеты. Перехватывают управление браузером пользователя.

Для защиты компьютера от вирусов необходимо соблюдать ряд основных мер:

- Установить на компьютер современную антивирусную программу и постоянно обновлять ее версии.
- При считывании с дискет информации, записанной на других компьютерах, обязательно проверять дискеты на наличие вирусов.
- Защищать свои дискеты от записи при работе на других компьютерах.
- Периодически проверять жесткие диски на наличие вирусов.
- Не запускать программу, если она вызывает подозрения.
- Проверять файлы, получаемые по сетям.
- Делать архивные копии на дискетах ценной информации.

Существует множество антивирусных программ, например, Norton AntiVirus, AVP, Doctor Web и др. Но эти программы должны выполнять ряд функций:

- Поиск подозрительных вирусных программ.
- Проверять системные файлы на появление изменений.
- Не допускать выполнение команд, посылаемых вирусами.
- Удалять вирусные программы из системы.
- Восстанавливать поврежденные вирусом файлы.

Во многих странах приняты законы о борьбе с компьютерными преступлениями, разработаны специальные программные средства защиты от компьютерных вирусов, тем не менее, количество компьютерных вирусов ежедневно растет.

***Вопросы для самоконтроля***

1. *Что входит в понятие компьютерный вирус?*
2. *Назовите разновидности компьютерных вирусов.*
3. *Какие защитные функции выполняют антивирусные программы?*

## 18. ТЕРМИНЫ И ОСНОВНЫЕ ПОНЯТИЯ

**Автоматизированная система управления** – понимается определенное количество компьютеров, промышленных контроллеров, устройств числового программного управления станками и промышленными роботами, устройств управления транспортными средствами и другими технологическими установками, объединенных локальными вычислительными сетями и обеспечивающих сбор, обработку, хранение и передачу управляющей информации.

**Алгоритм диагностирования** – совокупность предписаний, определяющих последовательность действий при проведении диагностирования.

**Апплеты** – прикладные программы, поддерживающие функциональные средства Web-узлов.

**Аутентификация** – подтверждение подлинности чего-либо, например, подлинности имени автора текста.

**Браузер** – программа, предназначенная для соединения с Интернетом и извлечения файлов с Web-узлов.

**Восстановление системы** – процесс перевода системы из неработоспособного состояния в работоспособное.

**Дефект** – любое несоответствие свойств системы ее свойствам заданным технической документацией.

**Идентификация** – совпадение каких либо двух событий, например, отождествление автора с разработанным им текстом.

**Исправное состояние системы** – состояние, при котором система соответствует всем требованиям нормативно-технической и проектной документации.

**Компьютерный вирус** – это программы или макросы, выполняющие некоторые, нежелательные для пользователя действия, препятствующие нормальной работе компьютера, разрушающие файловую структуру дисков и хранимую в компьютере информацию.

**Криптоанализ** характеризует раскрытие секретной или конфиденциальной информации.

**Криптограммой** называется зашифрованный при помощи специальных приемов текст или документ.

**Криптография** представляет собой совокупность методов преобразования информации, направленных на ее защиту от искажения или разглашения.

**Криптология** – наука о секретных (тайных) сообщениях.

**Криптосистема** обеспечивает работу АСУ с секретной или конфиденциальной информацией.

**Криптостойкость** оценивает способность зашифрованной информации противостоять криптоанализу.

**Надежность и безопасность АСУ**–защищенность от случайных или преднамеренных вмешательств в нормальный процесс ее функционирования, выражающийся в хищении или изменении информации, а также в нарушении ее работоспособности.

**Однонаправленной функцией** называется математическое выражение, не имеющее или имеющее бесконечное количество решений.

**Отказ внезапный** – отказ, характеризующийся скачкообразным изменениями значений одного или нескольких параметров системы.

**Отказ зависимый** – отказ, обусловленный другими отказами.

**Отказ конструкционный** – отказ, связанный с ошибкой конструктора или несовершенством принятых методов конструирования.

**Отказ независимый** – отказ, не обусловленный другими отказами.

**Отказ перемежающийся** – многократно возникающий самоустраняющийся отказ одного и того же характера.

**Отказ постепенный** – отказ, возникающий в результате постепенного изменения значений одного или нескольких параметров объекта.

**Отказ скрытый** – отказ, не обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования, но выявляемый при проведении технического обслуживания или специальными методами диагностики.

**Отказ технологический** – отказ, связанный с ошибкой при изготовлении, нарушении принятой технологии, несовершенством технологии.

**Отказ эксплуатационный** – отказ, связанный с нарушением правил эксплуатации; внешних воздействий, не свойственных нормальной эксплуатации.

**Отказ явный** – отказ, обнаруженный визуально или штатными методами и средствами контроля и диагностирования при подготовке объекта к применению или в процессе его применения по назначению.

**Работоспособное состояние системы** – состояние системы, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической и проектной документации.

**Резервируемый элемент** – основной элемент, на случай отказа которого в объекте предусмотрены один или несколько резервных элементов.

**Резервный элемент** – элемент, предназначенный для выполнения функций основного элемента в случае отказа последнего.

**Сбой** – самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора.

**Техническое состояние** – состояние, которое характеризуется в определенный момент времени, при определенных условиях внешней среды, значениями параметров, установленных технической документацией.

## ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Автоматизация типовых технологических процессов и установок: Учеб. для вузов/А.М.Корытин, Н.К.Петров, С.Н.Радимов, Н.К.Шапарев.-2-е изд.,перераб. и доп.-М.:Энергоатомиздат, 1988.-432с.: ил.
2. ГОСТ 27.002-89. Надежность в технике. Термины и определения.-М.: Изд-во стандартов,1989.-37с.
3. ГОСТ 20911-89. Техническая диагностика. Термины и определения.- М.: Изд-во стандартов,1989.-13с.
4. Кемпинский М.М. Точность и надежность измерительных приборов.-Л.: Машиностроение, 1972.-264с.
5. Михаэль А.Бэнкс. Информационная защита ПК/ Пер. с англ.: Киев: “ВЕК+”.-М.: “Энтроп”.-СПб.: “Корона-Принт”, 2001.- 269 с.: ил.
6. Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин. Защита информации в компьютерных системах и сетях /Под ред В.Ф.Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001.-376 с.: ил.
7. Технические средства диагностирования: Справочник/ В.В.Клюев, П.П.Пархоменко, В.Е.Абрамчук и др.; Под общ. ред. В.В. Клюева. -М.: Машиностроение, 1989.-672 с.

# ОГЛАВЛЕНИЕ

Сарвин Анатолий Александрович
Абакулина Людмила Ивановна
Готшальк Олег Алексеевич

Диагностика и надежность автоматизированных систем
Письменные лекции

Редактор М.Ю.Комарова

Сводный темплан 2003г.
Лицензия ЛР №020308 от 14.02.97

Подписано в печать Формат 60x84 1/16
Б.Кн.-журн. П.л. 4,5 Б.л. 2,25 РТП РИО СЗТУ
Тираж Заказ

Северо-Западный государственный заочный технический университет
РИО СЗТУ, член Издательско- полиграфической ассоциации
Вузов Санкт-Петербурга
191 186, Санкт-Петербург, ул.Миллионная, 5