ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ В ЭРГАСИСТЕМАХ

Ловцов Д.А.*

***Ключевые слова**: эргасистема, защищенность информации, достоверность, конфиденциальность, сохранность, принципы обеспечения, ошибки переработки, разрушающие факторы, несанкционированный доступ и использование, способы защиты информации, математические структуры.*

Аннотация.

Цель работы: совершенствование научно-методической базы теории защищенности информации в эргасистемах.

Метод: системный анализ, прагматическая классификация и математическое моделирование основных частных задач обеспечения защищенности информации в эргасистемах.

Результаты: обоснована непротиворечивая совокупность принципов контроля и защиты информации от ошибок переработки, разрушающих факторов и несанкционированного доступа и использования; обоснована прагматическая классификация ошибок при переработке информации, разрушающих факторов, потенциальных каналов утечки информации, а также соответствующих способов защиты информации; определены математические структуры моделей задач обеспечения достоверности, конфиденциальности и сохранности информации в эргасистеме; приведены доказательства утверждений о повышении достоверности информации, о совершенной семантической скрытности и об энергетической скрытности динамической информации.

Полученные результаты являются концептуальной основой для создания соответствующего эффективного информационно-математического обеспечения контроля и защиты информации в эргасистемах.

DOI: 10.21681/1994-1404-2021-1-36-50

Введение

Эффективность и информационная безопасность эргатических систем (эргасистем) в значительной степени определяются *защищённостью* циркулирующей и перерабатываемой в них содержательной информации, для обеспечения которой создаются и совершенствуются функциональные подсистемы контроля и защиты информации (КЗИ). При этом под ***защищённостью*** информации понимается конструктивное свойство функциональной подсистемы КЗИ, характеризующее степень защищённости информационных массивов (ИМ) и заключающееся в способности не допускать случайного или целенаправленного искажения или разрушения, раскрытия или модификации ИМ в информационной базе эргасистемы[1] [6, 7].

Существующие угрозы нарушения *защищённости* (в частности, достоверности, конфиденциальности и сохранности) информации обусловливают жизненно важную необходимость создания эффективных мер контроля всевозможных угроз и защиты содержательной информации в эргасистемах от искажения при переработке, от раскрытия (утечки) и модификации при несанкционированном доступе и использовании, а также от разрушения при эксплуатации [1].

Задача обеспечения (повышения) *достоверности* (помехоустойчивости, помехозащищенности [7]) при переработке информации в эргасистеме заключается главным образом в контроле правильности ИМ, обнаружении ошибок и их исправлении на различных этапах переработки информации. Задача обеспечения *конфиденциальности* (доступности, скрытности, имитостойкости [7]) — в контроле полномочий объектов эргасистемы (операторов, программно-технических средств и ресурсов эргасистемы), контроле операций по выборке ИМ и посылке данных на хранение, в установлении правил взаимодействий и разграничении доступа операторов. Задача обеспечения *сохранности*

[1] *Ловцов Д. А.* Методы защиты информации в АСУ сложными динамическими объектами // НТИ. Сер. 2. Информ. процессы и системы. 2000. № 5. С. 29–45.

* ***Ловцов Дмитрий Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: dal-1206@mail.ru

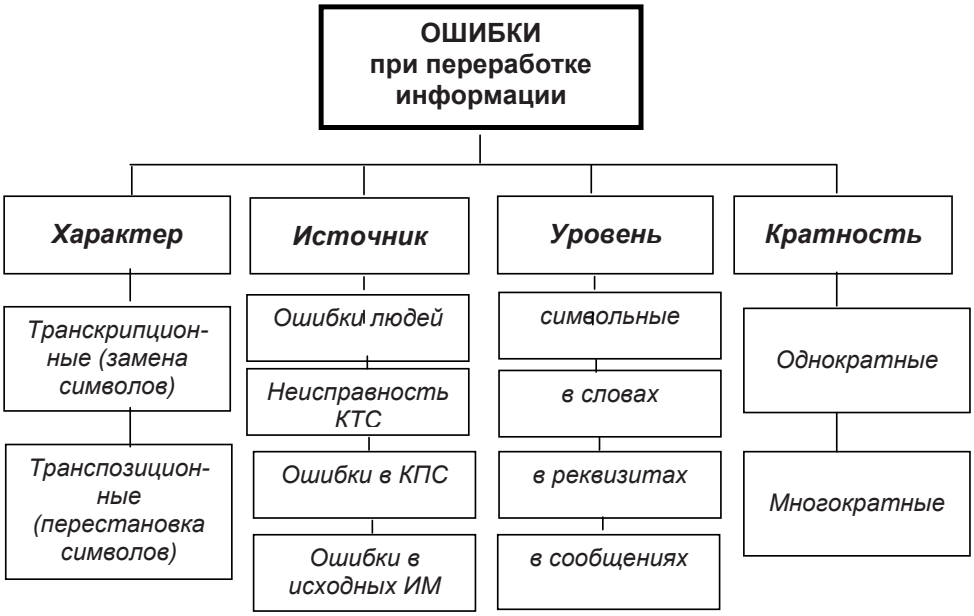


Рис. 1. Общая классификация ошибок, возникающих в эргасистеме при переработке информации

(целостности, готовности [7]) информации при эксплуатации эргасистем — в контроле правильности ИМ, обнаружении ошибок, резервировании (копировании, дублировании ИМ и их предысторий, т. е. предыдущих ИМ и массивов изменений), регенерации (перезаписи) ИМ, восстановлении ИМ во внутримашинной информационной базе по зарезервированным ИМ и ИМ из исходных документов (сообщений). Оптимальное резервирование ИМ является также одним из системных методов повышения *достоверности* информации в эргасистеме.

Совместное продуктивное решение данных сложных задач возможно на основе обоснованной непротиворечивой совокупности принципов КЗИ от ошибок переработки, от разрушающих факторов и от несанкционированного доступа и использования.

Принципы контроля и защиты информации от ошибок переработки

Исследование задачи *обеспечения достоверности информации* (ОДИ) в эргасистеме осуществляется на трех уровнях[2] [5, 14]:

синтаксическом (связан с контролем и защитой элементарных составляющих ИМ — знаков или символов);

семантическом (связан с обеспечением достоверности смыслового значения ИМ, их логичности, непротиворечивости и согласованности);

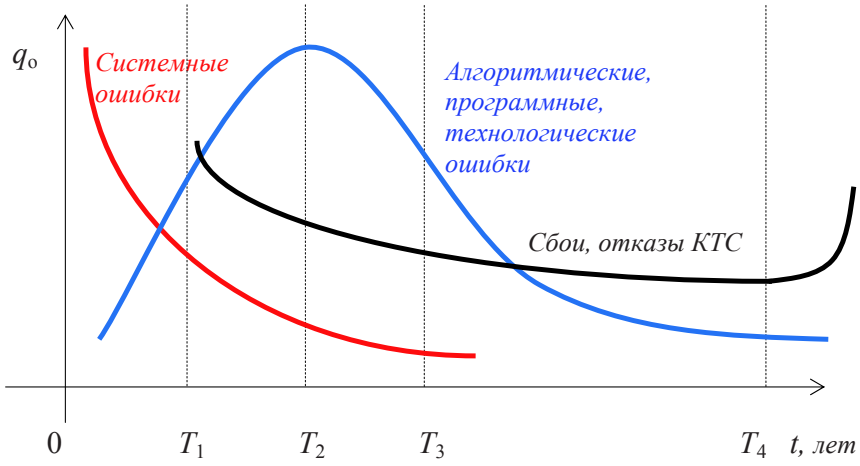
прагматическом (связан с изучением вопросов ценности информации при принятии управленческих решений, её доступности и своевременности, влияния ошибок на качество и эффективность функционирования эргасистем).

На *первом* (синтаксическом) уровне в качестве показателя достоверности можно использовать функцию $D = 1 - q_1$ (*верность* [5]) вероятности q_1 ошибки, т. е. события, состоящего в том, что *единичный* правильный (верный) символ или знак заменяется в процессе переработки информации другим, ошибочным.

На *втором* и *третьем* уровнях в качестве показателя достоверности можно использовать некоторую функцию $D(q_1)$ вероятности q_1 ошибки *единичного массива информации* (ЕМИ), т. е. события, заключающегося в том, что реальный ЕМИ (поле, запись, блок, дейтаграмма, ИМ, перфокарта, документ и др.) в информационной базе (ИБ) эргасистемы не совпадает (в пределах заданной точности) с его истинным значением.

Процесс переработки информации (реализации любой задачи в эргасистеме) можно разбить на ряд основных этапов: сбор и регистрация информации; передача исходной информации по каналам связи и первичная обработка ИМ, включая контроль обеспечения заданной достоверности; подготовка первичного документа для ввода в комплекс средств автоматизации (КСА); преобразование и перезапись данных на промежуточные документы; перезапись информации на машинный носитель; ввод информации в КСА (ЭВМ), в том числе непосредственный ввод в диалоговом человеко-машинном режиме; машинная обработка данных по алгоритмам, реализующим математические модели (решение задачи на КСА); сортировка выходных ИМ и их вывод из КСА на внешние устройства; сортировка полученных документов, их проверка и доставка получателям.

[2] *Мамиконов А. Г., Кульба В. В., Шелков А. Б.* Достоверность, защита и резервирование информации в АСУ. М. : Энергоиздат, 1986. 304 с.;
Мельников Ю. Н. Достоверность информации в сложных системах. М. : Сов. радио, 1974. 192 с.



Экспликация: T_1 — разработка проекта эргасистемы; (T_1 — T_2) — разработка эргасистемы; (T_2 — T_3) — ввод КСА в эксплуатацию; (T_3 — T_4) — гарантийная эксплуатация КСА; после T_4 — износ и старение КСА.

Рис. 2. Графики зависимости вероятности отказов на этапах жизненного цикла эргасистемы

Ошибки (*рис.* 1) могут возникать на любом из перечисленных этапов переработки информации. Ошибки персонала, операторов и пользователей средств автоматизации определяются [5]:

психофизиологическими характеристиками человека (усталостью и снижением работоспособности после определённого времени работы, неправильной интерпретацией используемых ИМ);

объективными причинами (несовершенством моделей представления информации, отсутствием должностных инструкций и нормативов, квалификацией персонала, несовершенством комплекса технических средств (КТС), неудачным расположением или неудобной конструкцией их с точки зрения эксплуатации);

субъективными причинами (небрежностью, безразличием, несознательностью, безответственностью некоторых операторов, следствием нарушения принципа материальной заинтересованности, преднамеренным искажением ИМ в корыстных целях, отсутствием должного контроля со стороны руководства за качеством выполняемых операций, плохой организацией труда и др.).

Ошибки, возникающие в процессе переработки информации на КСА, связаны [1] с помехами, сбоями и отказами КТС, ошибками в комплексах программных средств (КПС), недостаточной точностью или ошибками в исходных данных, округлением исходных, промежуточных и выходных данных, неадекватностью реализованных математических моделей реальным процессам, приближённым характером используемых методов решения задач на ЭВМ (что характерно в первую очередь для итерационных методов).

Неисправность КТС приводит к ошибкам, связанным с неисправностью центрального процессора КСА (ЭВМ), периферийного оборудования, несоответствием техническим нормам и условиям хранения магнитных носителей ИМ, физическим износом и старением элементов и узлов КТС и др. Вероятность q_o отказов КТС изменяется на этапах его жизненного цикла (*рис.* 2).

Ошибки в комплексах алгоритмов и программ обычно классифицируют на[3] [5] (см. *рис.* 2):

системные, обусловленные неправильным пониманием требований автоматизируемой задачи эргасистемы и условий её реализации;

алгоритмические, связанные с некорректной формулировкой и программной реализацией алгоритмов;

программные, возникающие вследствие описок при программировании на ЭВМ, ошибок при кодировании информационных символов, ошибок в логике машинной программы и др.;

технологические, возникающие в процессе подготовки программной документации и перевода её во внутримашинную информационную базу эргасистемы.

Обеспечение достоверности переработки информации в функционирующей эргасистеме состоит в определении пунктов логической обработки и контроля ИМ. На основе анализа различных структур переработки информации можно выделить несколько типовых структур.

В стандартном *типовом модуле переработки* (ТМП) цикл переработки информации распадается (*рис.* 3) на непосредственно логическую (математическую) обработку, контроль и исправление ошибок [5, 8]. На некоторых этапах переработки информации операции (фазы) контроля и исправления недостоверных ЕМИ могут отсутствовать либо осуществляться для группы

[3] *Ловцов Д. А.* Контроль и защита информации в АСУ. В 2-х кн. Кн. 1. Вопросы теории и применения. М. : ВА им. Петра Великого, 1991. 172 с. Кн. 2. Моделирование и разработки. М. : ВА им. Петра Великого, 1997. 252 с.

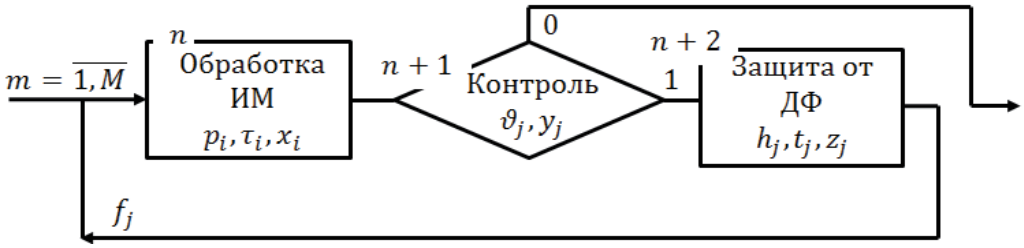


Рис. 3. Вариант разметки ТМП для задачи ОДИ

из нескольких этапов, на каждом из которых, в свою очередь, осуществляется локальный контроль и исправление ошибок. После исправления ошибочных ЕМИ они вновь обрабатываются с последующим контролем и исправлением. Фазы контроля и исправления ошибок могут повторяться *случайное* число раз.

В общем виде вероятность D достоверной переработки ЕМИ в эргасистеме определяется структурными параметрами $<G, p_i, f_j, I, J>$ технологического процесса переработки информации (ТППИ) и техническими параметрами $<\tau_i, x_i, \vartheta_j, y_j, t_j, z_j>$ алгоритмов (устройств) обработки на каждом этапе переработки информации:

$$D = 1 - Q = D\{S_1, \nu_m, C^0, T^0, M\}, \quad m=1,\ldots,M, \qquad (1)$$

где $S_1 = <G, p_i = 1 - q_i, f_j = 1 - e_j, \tau_i, x_i, \vartheta_j, y_j, t_j, z_j>, i = 1,\ldots,I; j = 1,\ldots,J$ — структура переработки информации; ν_m — значение случайной величины — количества циклов обработки m-го ЕМИ; C^0 — заданный материальный ресурс на обработку, контроль и исправление ошибочного ЕМИ; T^0 — директивное время переработки информации; Q, M — вероятность искажения и величина массива перерабатываемой информации соответственно.

В эргасистеме, как правило, добиваться теоретически максимальной достоверности переработки информации нецелесообразно из-за резкого повышения сложности эргасистемы, стоимости её разработки, внедрения и эксплуатации; достаточно обеспечить требуемый (допустимый) уровень достоверности D. В реальных эргасистемах требуемая достоверность устанавливается с учётом последствий, к которым могут привести возникшие ошибки, и тех затрат (материальных, временных, интеллектуальных и др.), которые необходимы для их предотвращения (табл. 1).

Вместе с тем КТС эргасистемы часто не обеспечивает требуемого уровня достоверности переработки ИМ. Например, существующие каналы связи в эргасистеме обеспечивают (в условиях помех типа «белый шум» и с учётом различных значений удельного расхода β^2 энергии сигнала-переносчика ИМ и методов телеграфии: амплитудной — АТ, частотной — ЧТ, фазовой — ФТ, относительной фазовой — ОФТ) обмен информацией с вероятностью искажения 1 бит (рис. 4):

$q_1 \geq (10^{-1} \ldots 10^{-2})$ — радиоканал;
$q_1 \geq (10^{-3} \ldots 10^{-4})$ — радиорелейный канал;

Таблица 1

Вероятность ошибки и уровень затрат на ОДИ для некоторых классов задач эргасистемы

Класс задач эргасистемы	Допустимая вероятность q_1 искажения ЕМИ (ошибки)	Временные и материальные затраты, %				
		Время t_1 на техн. проектирование	Время t_2 на программирование	Время t_3 работы программы	Объем C_1 памяти	Стоимость C_1 КТС и др.
Оперативное планирование	10^{-4}	100	100	100	100	100
Технико-экономическое планирование	10^{-5}					
Статистический учет	10^{-5}					
Бухгалтерский учет	10^{-6}					
Обработка контрольно-измерительной информации от СДО	10^{-8}	150	150	160	170	150–200
Выработка управляющих воздействий на СДО	10^{-9}					

$q_1 \geq (10^{-4} \ \ldots \ 10^{-5})$ — проводной канал.

Поэтому для достижения *требуемой* $(q_1 \leq 10^{-6} \ldots 10^{-9})$ или *максимальной* достоверности переработки информации в эргасистеме используются специальные средства, методы и их комбинации, в том числе *каналы передачи данных* (см. рис. 4), содержащие устройства повышения достоверности (защиты от ошибок переработки).

В принятых обозначениях математическую *постановку задачи обеспечения достоверности* информации как задачи поиска оптимальной структуры $S_1^* \in \Delta_1$ переработки информации, минимизирующей суммарное (на обработку, контроль и исправления ошибок) время T и/или материальные затраты C на переработку информации, при ограничении на достоверность D перерабатываемых ИМ и при условии независимости вероятностей искажения q_i и обнаружения f_j ошибок информационных элементов можно записать в виде:

$$K_1\colon D(S_1^*, M, \tau_i, x_i, \vartheta_j, y_j, t_j, z_j, \nu_m) \geq D^0 \qquad (2)$$
$$T(S_1^*, M, \tau_i, \vartheta_j, t_j, \nu_m) = \min_{\{S1\}},$$
$$C(S_1^*, M, x_i, y_j, z_j, \nu_m) = \min_{\{S1\}},$$

где $\{S_1\} = \Delta_1$ — множество допустимых структур $S_1 = <p_i, f_j, I, J>$ переработки информации; D^0 — заданное значение вероятности достоверной переработки ЕМИ в эргасистеме.

Для стандартного ТМП (см. рис. 3) при $I = J = 1$ и заданных $p, f, \tau, \vartheta, t, x, y, z, C^0, T^0$ единственным параметром оптимизации процесса обработки ИМ является количество циклов ν_m, $m = 1, \ldots, M$ проверки и исправления ошибочной информации.

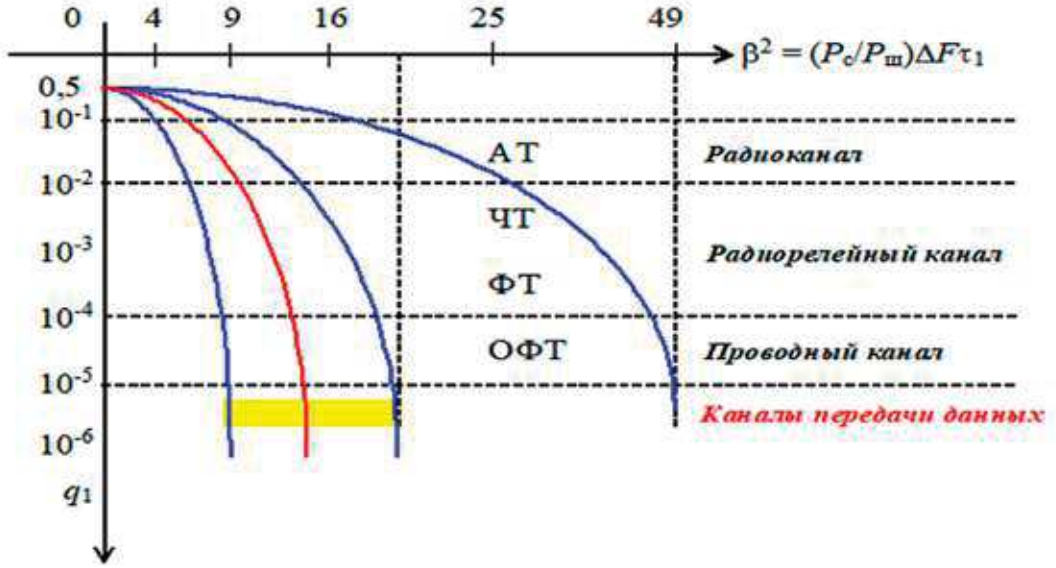


Рис. 4. Зависимость удельного расхода энергии сигнала-переносчика ИМ и вероятности искажения символа

Производными стандартного ТМП являются последовательная структура переработки информации, последовательная структура при N-кратной переработке информации, последовательная структура при N-кратной переработке информации с общим контролем (общей обратной связью), циклическая и последовательно-циклическая структуры, сеть переработки информации[4]. *Сетевую* структуру переработки информации можно представить в виде графа, множество дуг которого образует стандартные ТМП и сложные циклы, а множество вершин совпадает с начальными и (или) конечными точками сложных циклов и стандартных ТМП.

***Утверждение* 1.** Достоверность информации в эргасистеме с последовательной структурой ТППИ и контролем в каждом узле по принципу обратной связи повышается, если концы обратной связи перенести к началу информационной цепи технологических операций[5].

Доказательство. Возможны три различных варианта (рис. 5, а, б, в) минимальных структурных фрагментов, из которых, собственно, и составляется структура (сеть) ТППИ в целом: (а) последовательное соединение двух ТМП, (б) последовательное соединение двух ТМП с общей обратной связью и без обратной связи для второго модуля, (в) последовательное соединение двух ТМП с общей обратной связью. Для простоты символ «решение» на рис. 5 изображен в виде точки.

[4] *Ловцов Д. А.* Контроль и защита информации в АСУ. В 2-х кн. Кн. 1. Вопросы теории и применения. М. : ВА им. Петра Великого, 1991. 172 с. Кн. 2. Моделирование и разработки. М. : ВА им. Петра Великого, 1997. 252 с.

[5] *Ловцов Д. А., Князев А. Г.* Оптимизация структуры достоверной переработки информации // НТИ. Сер. 2. Информ. процессы и системы. 1998. № 10. С. 20–27.

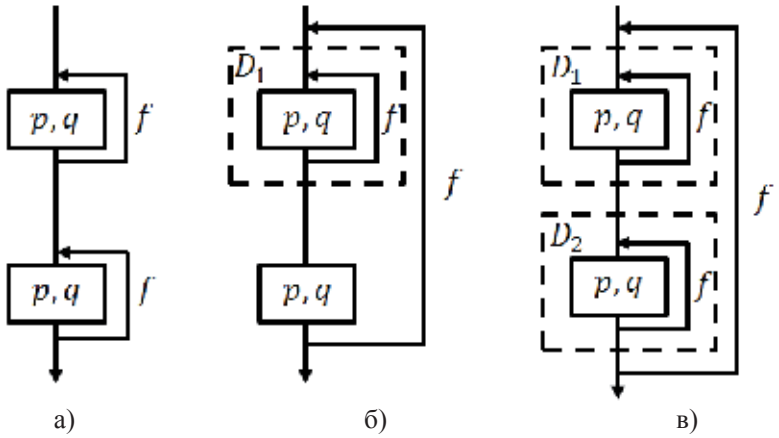


Рис. 5. Варианты минимальных структурных фрагментов

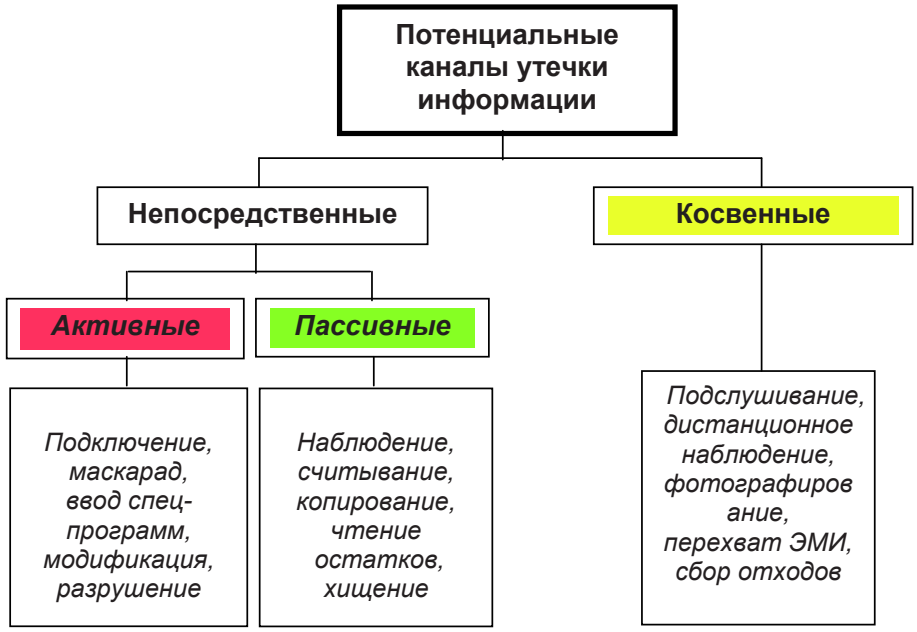


Рис. 6. Классификация каналы утечки информации

Определим для каждого из них вероятности того, что в установившемся режиме на k-м двухфазном $(i = 1,\ldots,2)$ этапе ТППИ единичный массив будет переработан без ошибок (при условии p, q, f = const):

$$D_а = D_{i=1}D_{i=2} = [p/(1 - qf)]^2 = p^2/(1 - 2qf + qf\boldsymbol{qf}), \quad (3)$$

$$D_б = D_1 p/[1 - (1 - D_1 p)f] = \\ = p^2/[1 - 2qf + qf(\boldsymbol{f + q - 1})], \quad (4)$$

$$D_1 D_2/[1 - (1 - D_1 D_2)f] = \\ = p^2/\{1 - 2qf + qf[(\boldsymbol{f + q - 1}) + \boldsymbol{f + qf - qf^2 - 1}]\}. \quad (5)$$

Из выражений (3) — (5) видно (выделено жирным), что поскольку $qf \geq f + q - 1 \geq f + q - 1 + f + qf - qf^2 - 1$, то $D_а \leq D_б \leq D_в$, что и требовалось доказать.

Следовательно, первый структурный фрагмент является наименее приемлемым по критерию (2), но, с другой стороны, его реализация приводит к наименьшим временным и материальным затратам, поскольку $T_а < T_б < T_в$, $C_а < C_б < C_в$.

Принципы контроля и защиты информации от несанкционированного доступа и использования

Защищенность ИМ в значительной степени зависит от принятия эффективных мер по закрытию потенциальных *каналов утечки информации*, под которыми понимают[6] [9] объективно существующие способы несанкционированного использования данных, обусловленные структурно-функциональными особенностями эргасистем.

Множество существующих каналов утечки информации в эргасистеме можно разделить на три больших группы (рис. 6):

[6] *Ловцов Д. А.* Защита информации в информационно-вычислительной сети // НТИ. Сер. 3. Информ. процессы и системы. 1997. № 2. С. 7–13; Ловцов Д. А. Введение в информационную теорию АСУ: Монография. М. : ВА им. Петра Великого, 1996. 434 с.

непосредственные активные каналы, связанные с контактным несанкционированным доступом (НСД) к ресурсам эргасистемы и изменением её компонентов;

непосредственные пассивные каналы, связанные с контактным НСД к ресурсам эргасистемы, но не предусматривающие изменений компонентов системы;

косвенные каналы, позволяющие осуществить неконтактный НСД к ресурсам эргасистем.

К *первой* группе относятся, в частности, следующие основные каналы утечки информации: незаконное подключение к КТС (терминалам ввода-вывода, линиям передачи данных и др.); маскировка под зарегистрированных операторов (маскарад); несанкционированное изменение машинных программных массивов; несанкционированный ввод в программное обеспечение эргасистемы программных «закладок», специально разработанных для осуществления НСД к ИМ; злоумышленный вывод из строя подсистемы КЗИ от НСД и др.

Ко *второй* группе относятся следующие каналы: наблюдение за информационными массивами в процессе их переработки в эргасистеме; копирование ИМ, хранящихся на машинных (магнитных, оптических и др.) и немашинных (документальных) носителях; прямое хищение материальных носителей информации; преднамеренное считывание ИМ в файлах других операторов; сбор (чтение) остаточной информации на регистрах и в полях запоминающих устройств; использование служебного положения, т. е. незапланированного просмотра (ревизии) ИМ сотрудниками эргасистемы.

Каналы *третьей* группы: применение подслушивающих устройств; дистанционное наблюдение или фотографирование ИМ, представленных в визуальной (на экране дисплея, табло), графической или документальной форме; перехват, расшифровка и регистрация электромагнитного излучения (ЭМИ) КТС в процессе переработки информации (наличие большого количества переключательных цепей в составе современных ЭВМ позволяет в определенных условиях регистрировать их работу на значительном удалении как маломощного коротковолнового передатчика) с помощью специально разработанных для этой цели технических средств; сбор отходов («мусора») производства и функционирования эргасистем.

Непосредственное проникновение в информационную базу эргасистемы может осуществляться скрытно, т. е. в обход контрольных программ обеспечения конфиденциальности информации (ОКИ), а также с помощью нетрадиционных *скрытых каналов* [10, 11], реализуемых с помощью встроенных аппаратно-программных «закладок».

Наиболее характерные традиционные приёмы проникновения[7]:

использование точек входа, установленных в КСА программистами и обслуживающим персоналом, или точек, обнаруженных при проверках цепей системного контроля;

подключение к сети передачи данных специального терминала, обеспечивающего вход в информационную базу эргасистемы путем пересечения линии связи законного оператора с последующим восстановлением связи по типу ошибочного сообщения, а также в момент, когда оператор не проявляет активности, но продолжает занимать канал передачи данных;

аннулирование сигнала оператора о завершении работы с КСА и последующее продолжение работы от его имени;

неавторизованная модификация хранящейся информации, в результате чего оператор, которому эта информация принадлежит, не может получить к ней доступ.

Наибольшее распространение получили *скрытые каналы* по времени (используют временну́ю модуляцию занятости разделяемого информационно-вычислительного ресурса), каналы по памяти (используют разделяемый ресурс как промежуточный буфер при передаче данных), каналы в базах данных и знаний [4, 16] и ТППИ (используют зависимости между данными и их *функционально-технологическими преобразованиями*[8]).

Обеспечение гарантированной защиты эргасистем от НСД по скрытым каналам возможно при использовании «туннелирования» стандартных протоколов с использованием протоколов с минимальной избыточностью, не позволяющих модулировать поток пакетов. При этом пакеты стандартного протокола должны инкапсулироваться в пакеты протокола «туннелирования».

Основными *способами* ОКИ в эргасистеме являются (*рис*. 7): препятствие; контроль; управление доступом; преобразование информации.

Первый способ заключается в создании физического препятствия на пути к защищаемой информации и организации персонального автоматического (по индивидуальным токенам, жетонам, картам или ключам) и дистанционного (по специальным кодам) допуска к КСА.

Второй способ защиты заключается в организации всестороннего контроля законности операций (особенно копирования ИМ) ТППИ в эргасистеме, включая *надёжность* работы программно-математического обеспечения (ПМО), КТС и персонала; контроля законности получения доступа к ИМ каждого объекта (оператора, терминала, файла, программы или её части и др.) с целью предупреждения или обеспечения своевременной реакции на нарушение и защиты информации как от неавторизованного использования, так и от несанкционированного обслуживания системой.

Контроль доступа к информации эргасистем реализуется последовательным применением трёх способов (процедур) [3]:

[7] *Шураков В. В.* Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1987. 272 с.

[8] *Князев В. В., Ловцов Д. А.* Ситуационное планирование защищённой переработки информации в АСУ испытаниями сложных динамических объектов // Автоматика и телемеханика. 1998. № 9. С. 166–181.

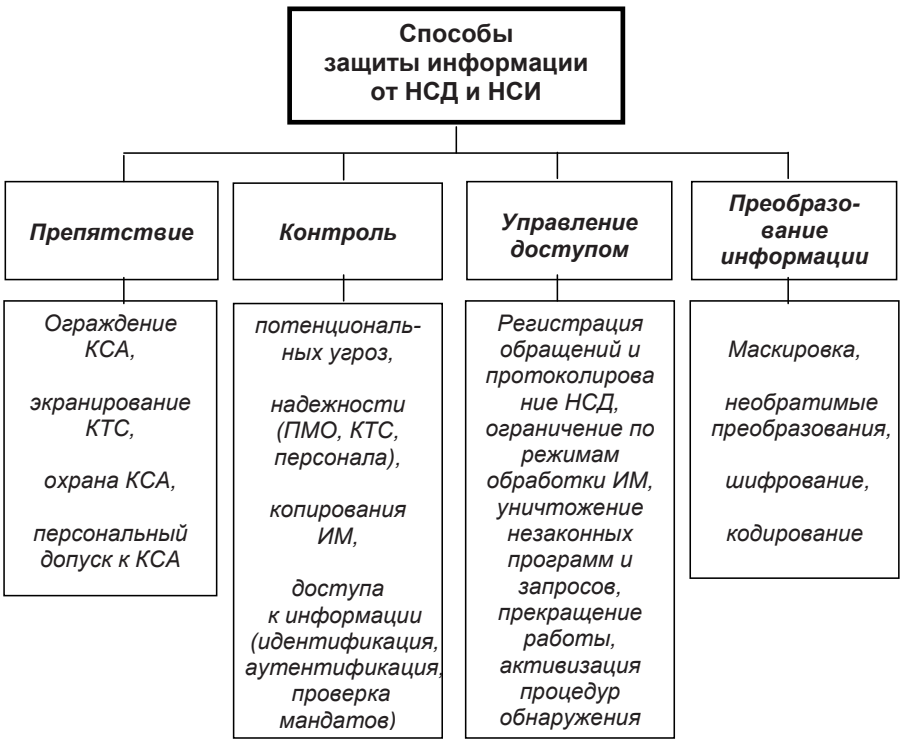


Рис. 7. Классификация способов защиты информации от несанкционированного доступа и использования

идентификации (присвоения объектам эргасистемы конкретных имён, кодов или их биометрических параметров [12] с целью последующего опознания и учёта фактов обращения, объединяемых в виде записей в так называемой «таблице авторизации», которая хранится в памяти КСА в преобразованном виде);

установления аутентичности (проверки подлинности объекта с помощью определенной информации, содержащейся в «матрице доступа» — списке операторов и запрещаемых объектов — и позволяющей убедиться в истинности обращения);

проверки полномочий (проверки информации, содержащейся в «матрице полномочий» по каждому объекту, о допустимых процедурах со стороны запрашиваемого).

Третий способ (см. рис. 7) ОКИ заключается в регулировании использования всех информационных и программно-технических ресурсов системы в пределах установленного регламента, включая ограничения на обработку ИМ, содержащих важную информацию, с уничтожением программ, сформулировавших незаконный запрос-обращение к особо важным ИМ или прекращением работы. При этом осуществляется регистрация всех (удачных и неудачных) обращений и протоколирование попыток НСД для последующего анализа и принятия мер при наличии угроз.

Четвёртый способ защиты (см. рис. 7) применяется для обеспечения необходимой скрытности информации как при переработке и хранении ИМ, так и при организации информационного обмена для получения допуска к ресурсам эргасистемы, а при передаче особо важной информации является единственным способом надежной защиты. Способ имеет четыре разновидности: маскировка; «необратимые» (плохообратимые) преобразования; шифрование; кодирование.

В случае *маскировки* защищаемые ИМ преобразуются таким образом, чтобы их содержание было доступно лишь при предъявлении некоторой специфической информации и осуществления обратных преобразований. При этом скрывается сам факт наличия информации.

В результате *«необратимых» преобразований* ИМ реформируются настолько, что для их раскрытия требуется применять специальный КТС.

Шифрование и *кодирование* позволяют скрывать содержание (смысл) ИМ при помощи, как правило, алфавитно-цифровых шифров (для донесений, отчётов и др.) и цифровых кодов (для команд, сигналов и др. коротких сообщений соответственно). При этом остается *проблемой* оценка уровня надежности и криптостойкости [15] (необратимости с точки зрения извлечения как корней, так и логарифмов) используемых стандартизованных односторонних функций зашифрования (дискретного возведения в степень в модульной арифметике) в различных криптоалгоритмах в условиях роста производительности современных вычислительных средств, приближающейся к условному порогу, равному приблизительно 10^{40} *операций в секунду* (и, возможно, более, если верить иностранным источникам, что существуют вычислительные возможности обеспечения обратимости стандартизованных функций зашифрования) [13].

Рассмотренные меры по защите ИМ предъявляют существенные *требования* к подсистеме КЗИ от несанкционированного доступа (НСД) и несанкционированного изменения (НСИ)[9]:

обеспечение свободного ввода данных в ИМ, к которым оператор имеет право доступа, и возможности спецификации доступа отдельных лиц к его информации с указанием типа разрешаемой работы;

обеспечение возможности выполнения процедур обновления и обработки ИМ, а также создания, модификации или исключения данных операторов в тех областях, за которые они отвечают;

информация, программное обеспечение и коммуникации должны быть защищены даже в случае серьёзных сбоев и отказов программных или технических средств;

зарегистрированный оператор должен всегда иметь доступ к своим индивидуальным ИМ;

защитный механизм КСА не должен быть разрушен даже при условии, что оператор обладает знаниями о технологии [2] его функционирования;

время реакции КСА на запросы оператора с учётом работы защитного механизма должно быть психологически приемлемым ($t \leq 20$ с);

подсистема ОКИ (в частности, подсистема авторизации, т. е. разрешения доступа) должна налагать допустимые ограничения на работу операционной системы КСА, структуру файлов, КТС и систему разделения времени;

обеспечение возможности выявления и использования минимально допустимого списка паролей, ключей и специальных команд с целью упрощения загрузки оператором при допустимых требованиях к ОКИ.

Создание подсистем КЗИ от НСД и НСИ включает три направления работ[10]: теоретические исследования; разработка средств защиты; обоснование способов использования средств защиты в эргасистеме.

В теоретическом плане основное внимание уделяется исследованию уязвимости информации в эргасистемах, выявлению и анализу каналов утечки информации, обоснованию принципов контроля и защиты информации в крупномасштабных эргасистемах и разработке методик оценки качества (надёжности) защиты. Общих методов решения проблемы ОКИ пока нет, достаточно строгие и практически значимые решения получены в настоящее время только для отдельных частных вопросов (выбор оптимальной длины пароля и оптимальной структуры ключа защиты, оценка стойкости шифрования и др.), для которых удалось сформулировать математически корректные постановки задач. Фундаментальными результатами теории ОКИ считаются *доказательства* сильной уязвимости информации в эргасистеме, возможности её защиты (с относительной надёжностью) и необходимости комбинированного использования всех способов, мер, методов, средств и мероприятий защиты.

***Утверждение* 2.** Необходимым и достаточным условием совершенной семантической скрытности динамической информации (передаваемых ИМ) в информационно-распределительной сети эргасистемы является равенство для всех переданных преобразованных информационных массивов (ПИМ) $M_{1i}, i=1,\ldots,N$ апостериорных вероятностей $p(M_{0i}|M_{1i})$ независимо от величины последних, т. е.:

$$p(M_{0i}|M_{1i}) = p(M_{0i}),\ i=1,\ldots,N, \qquad (6)$$

что эквивалентно независимости переданных ПИМ M_1 от передаваемых ИМ M_0.

Доказательство. Согласно теореме гипотез Байеса совместная вероятность передаваемых ИМ $p(M_{0i}),\ i=1,\ldots,N$, и переданных ПИМ $M_{1i},\ i=1,\ldots,N$

$$P(M_1, M_0) = P(M_0)P(M_1|M_0) = P(M_1)P(M_0|M_1).$$

Преобразуя формулу Байеса, получим:

$$-\log_2 P(M_0) - \log_2 P(M_1|M_0) =$$
$$= -\log_2 P(M_1) - \log_2 P(M_0|M_1).$$

Или, переходя к энтропии:

$$H(M_0) + H(M_1|M_0) = H(M_1) + H(M_0|M_1).$$

Тогда по «перехваченному» ПИМ M_1 соперник может получить информацию в количестве $I(M_1, M_0) = H(M_0) - H(M_0|M_1)$ *двед*. Для того чтобы обеспечить $I(M_1, M_0) = 0$, необходимо и достаточно, чтобы $H(M_0) = H(M_0|M_1)$ или, соответственно, $P(M_0) = P(M_0|M_1)$, что и требовалось доказать.

На практике для обеспечения условия (6) используются различные приёмы, в частности, так называемый способ «бегущего ключа», при котором поддерживается равенство скоростей V_{M1} передачи ПИМ M_1 и V_K передачи ключа K семантического преобразования $F(K)$ в ПИМ M_1, т. е.: $F(K)$: $M_0 \to M_2$.

***Утверждение* 3**. Необходимым и достаточным условием *энергетической* скрытности динамической информации (передаваемых ИМ) в информационно-распределительной сети эргасистемы является равенство

$$B >> (10...20), \qquad (7)$$

т. е. достаточно большая база $B = FT$ сигнала-переносчика ИМ M_0 длительностью T в полосе частот F, определяемая значением *удельного расхода* мощности $\beta^2 = (10...20)$, обеспечивающем необходимую (для каналов передачи данных) *верность* $q_1 \leq 10^{-5}$ приёма (см. рис. 4).

Доказательство. Искусственное увеличение полосы F частот согласно (7) позволяет уменьшить спектральную плотность (отношение мощности к полосе $N_с = P_с/F$ сигнала так, чтобы обеспечивалось неравенство $N_с << N_ш$, где $N_ш = P_ш/F$, и тем самым замаскировать сам факт передачи сигнала-переносчика ИМ M_0 в канале связи. При этом

$$\beta^2 = N_с/N_ш = P_с T/N_ш = P_с TF/N_ш F = (P_с/P_ш)B.$$

Отсюда: $P_с/P_ш = \beta^2/B \approx (10...20)/B$, т. е. для того чтобы обеспечить $P_с/P_ш << 1$, необходимо и до-

[9] *Шураков В. В.* Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1987. 272 с.

[10] *Ловцов Д. А.* Введение в информационную теорию АСУ : монография. М. : ВА им. Петра Великого, 1996. 434 с.

статочно обеспечить $B >> (10...20)$, что и требовалось доказать.

На практике для обеспечения условия (7) в качестве сигнала-переносчика используются так называемые сложные шумоподобные сигналы, обладающие большой избыточностью по полосе частот и длительности (например, с линейно-частотной модуляцией: $f_c = kt+f_0;\ F = k/T >> 1/T \rightarrow FT >> 1$), для которых T — длительность, соответствующая одному элементу $M_{1i} \in M_1$, $i=1,\ldots,N$ ПИМ, а F — полоса занимаемых частот. При использовании таких сигналов удается замаскировать их «белым» флуктуационным шумом с интенсивностью N_0 без ухудшения качества передачи сообщений (ИМ).

В разработке конкретных средств, методов и мероприятий защиты достигнуты наибольшие результаты, с помощью которых можно обеспечить требуемый уровень конфиденциальности ИМ в эргасистеме.

Отдельные разработки доведены до организации серийного выпуска или реализованы в виде общегосударственного стандарта. Например, ЭВМ, серийно выпускаемые американской фирмой IBM, содержат следующие средства защиты: схемы прерывания, позволяющие физически отделить исполнение программы оператора от исполнения управляющих процедур; блок защиты памяти, позволяющий контролировать и регулировать доступ оператора и задач к защищаемым полям памяти; специальные регистры защиты; программно-читаемые часы для регистрации времени свершения тех или иных событий и др.

В большинстве операционных систем современных ЭВМ предусматривается разграничение доступа к ИМ с помощью специальных паролей, четкое разделение ресурсов между решаемыми задачами, протоколирование информационно-вычислительного процесса и др.

Основные результаты, достигнутые в третьем направлении работ? — в обосновании способов использования методов, средств и мероприятий КЗИ от НСД и НСИ, — сводятся к следующим *выводам*:

ни один из способов, методов, мер, средств, мероприятий не является абсолютно надёжным, максимальный эффект достигается при объединении всех их в единую целостную подсистему ОКИ;

технические методы, меры и средства составляют лишь незначительную часть (около[11] 20%) подсистемы ОКИ (основную её часть составляют организационные);

подсистема ОКИ должна создаваться параллельно с эргасистемой, начиная с момента выработки общего замысла построения и проектирования последней;

выбор количества и содержания мероприятий ОКИ, а также способов их реализации осуществляется в каждом конкретном случае исходя из имеющихся средств и методов применительно к определённому КСА;

функционирование подсистемы ОКИ должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов переработки информации в эргасистеме;

необходимо осуществлять постоянный контроль функционирования подсистемы ОКИ со стороны администратора безопасности информации.

Набор $S_2 \in \Delta_2$ атрибутов доступа к ресурсам эргасистемы включает, в частности, множество $\Pi = <\Pi_1, \Pi_2,..., \Pi_n>$ индивидуальных *паролей* $\Pi_i = \{x_{ij}\}$, $i=1,\ldots,n;\ j=1,\ldots,w_i$ (имён, алгоритмов, вопросов и др.) n объектов эргасистемы; множество $Э = <Э_1, Э_2,...,Э_n>$ соответствующих эталонных паролей, преобразованных с целью защиты по соответствующему ключу $k \in K$ и хранящихся в специальной памяти эргасистемы; множество алфавитов $A=\{A_1(R_1), A_2(R_2),...,A_L(R_L)\}$ различного размера R_l, $l=1,\ldots,L$ парольных символов $x_{ijl} \in A_l(R_l)$; определённое значение длительности цикла доступа $T = <t_и, t_x, t_о, t_п, t_з>$, включающей, в частности, время $t_и$ ввода имени объекта эргасистемы и время t_x ввода пароля, время $t_о$ отключения КСА в случае ошибочного (неверного) ввода, $t_п$ — печати сообщения об ошибке, $t_з$ — искусственной задержки начала следующей попытки; заданное значение числа f разрешённых попыток доступа.

В принятых обозначениях общую математическую постановку *задачи обеспечения конфиденциальности информации* как задачи поиска оптимального набора $S = <\Pi, Э, K, A, T, f>$ атрибутов доступа, минимизирующего сумму $\Sigma_j c_j$ потерь от раскрытия (утечки) информации и затрат на разработку и эксплуатацию элементов КЗИ при ограничении на вероятность p_w НСД (раскрытия пароля) и на ожидаемое время $\check{T}_o$ безопасной работы, можно записать в виде:

$$\begin{aligned} &K: \Sigma_j c_j(S_2^*) = \min_{\{S2\}}, \\ &\quad p_w(S_2^*) \le p_w^0, \\ &\quad \check{T}_o(S_2^*) > \check{T}_o^0, \\ &\quad \Sigma_j c_j = c_1 + \check{c}_2 = c_1 + g(1 - p_w), \end{aligned} \tag{8}$$

где c_1 — затраты, связанные с разработкой и эксплуатацией элементов КЗИ; $\check{c}_2$ — математическое ожидание потерь, которое несёт эргасистема в результате раскрытия привилегированной информации; g — моральные и материальные потери эргасистемы от НСИ.

Решение задачи (8) возможно на основе известных методов математического программирования.

Принципы контроля и защиты информации от разрушающих факторов

Причины, вызывающие разрушение ИМ на физических магнитных носителях информации (МНИ), подразделяются на технологические и эксплуатационные, по наличию дефектов на МНИ. Технологические разрушающие факторы обусловлены показателями качества МНИ, несовершенством их производства, вследствие чего эти носители имеют заводские дефекты (повреждения магнитного слоя, надрывы кромки лент и др.).

[11] Ловцов Д. А. Введение в информационную теорию АСУ : монография. М. : ВА им. Петра Великого, 1996. 434 с.

Таблица 2

Эксплуатационные причины разрушения ИМ

Результат воздействия разрушающих факторов	Разрушающие факторы	
	Режим эксплуатации	
	Хранение ИМ на носителях	Непосредственное использование ИМ
Разрушение информационного массива	1. Ошибки персонала архивов МНИ. 2. Ошибки операторов КСА. 3. Агрессивность среды (температура, влажность, ЭМИ, помехи и др.).	1. Ошибки оператора КСА и пользователя (неправильная установка МНИ, повторные прогоны данных, использование не тех программ, запуск работы с неверного места, неправильный ввод задания и др.). 2. Несанкционированные и ошибочные корректировки пользователем записей и данных. 3. Деструктивные действия компьютерных вирусов. 4. Ошибки (всех видов) в КПС. 5. Сбой (отказ) КСА, ЭВМ, МНИ (не механической части) из-за скачков напряжения в сети питания, неисправностей энергоснабжения и др.). 6. Динамический перекос головок МНИ. 7. Катастрофический отказ ЭВМ, каналов связи и передачи данных, МНИ (случайное включение стирающей головки).
Разрушение магнитного носителя	1. Ошибки персонала КСА. 2. Износ МНИ (КТС). 3. Отпечатки на магнитной поверхности (FeO). 4. Вытягивание и продольное коробление (сабельность) МНИ.	1. Неправильное обращение с МНИ обслуживающего персонала. 2. Скол магнитной поверхности. 3. Обрыв, сдвиг витков или неровная намотка магнитных лент. 4. Глянцевые пятна, потертость или царапины на магнитной поверхности. 5. Неисправность лентопротяжных механизмов МНИ (механических частей). 6. Неисправность контроллеров МНИ, КТС.

Эксплуатационные разрушающие факторы (табл. 2) обусловлены неправильной (некомпетентной или недобросовестной) эксплуатацией МНИ и КСА в целом[12], в результате чего возможны механические повреждения, приводящие к выпадению сигналов при записи-считывании, искажения, модификация, разрушение ИМ и др.

Естественный износ МНИ (см. табл. 2) носит характер старения, когда с течением времени (5–10 лет и более) характеристики МНИ претерпевают «возрастные» изменения, приводящие к невозможности использования информации. Износ и старение, в частности, магнитных лент, широко используемых в архивах и дата-центрах, являются основными причинами потери информации при длительном хранении [5]. Увеличить срок сохранности ИМ можно, используя специальные процедуры чистки магнитных лент, их проверки и регенерации.

Проверка ИМ — процедура контроля путем записи-считывания информации для определения количества и местоположения ошибок. Если имеется возможность проверки ИМ и исправления искаженной информации, применяются специальные тестовые процедуры контроля, позволяющие уменьшать количество ошибок [5].

Регенерация ИМ — процедура перезаписи информации со старого МНИ на новый. При этом существует *рациональный* (оптимальный, удовлетворительный) *период* регенерации, при котором достигается минимум суммарных затрат на перезапись и потерь от уничтожения хранимой информации. В методах определения рациональных периодов регенерации ИМ используются известные[13] модели оптимизации регламентных и профилактических мероприятий.

При увеличении масштабов и сложности эргасистем усложняется работа операторов и организация разграничения доступа к ИМ и программно-техническим ресурсам. Поэтому возрастает доля разрушения информации вследствие ошибок операторов (использование ИМ не по назначению и др.) и несанкционированных корректировок. Ошибки операторов на этапе ввода и размещения исходных данных являются наиболее опасными, поскольку часто их обнаружение становится возможным спустя долгое время после их появления. Кроме того, операторы, имеющие доступ к ресурсам КСА, могут злонамеренно составить и использовать специальную машинную программу (ком-

[12] *Иыуду К. А.* Надёжность, контроль и диагностика вычислительных машин и систем. М. : Высшая школа, 1989. 216 с.

[13] Герцбах И. Б. Модели профилактики. М. : Сов. Радио, 1973. 250 с.

Рис. 8. Классификация способов и средств резервирования информационных массивов

пьютерный вирус и др.) для искажения или разрушения информационно-программного обеспечения КСА.

Способы резервирования ИМ с целью обеспечения сохранности информации включают (рис. 8):

оперативное (краткосрочное) резервирование — создание и хранение резервных рабочих копий и (или) *предысторий* ИМ, используемых только для решения функциональных задач эргасистемы;

восстановительное резервирование — создание и хранение дополнительных резервных (восстановительных) копий и (или) предысторий ИМ, используемых только для восстановления разрушенных рабочих копий и (или) предысторий ИМ;

долговременное (долгосрочное) резервирование — создание, длительное (десятки лет и более) хранение и обслуживание архивов оригиналов, дубликатов, резервных копий и (или) предысторий ИМ, используемых только для получения и восстановления разрушенных рабочих и дополнительных (восстановительных) копий и (или) предысторий ИМ.

Задачами *оперативного* резервирования ИМ являются определение (расчет) оптимального числа копий и (или) предысторий, обеспечивающих:

максимизацию коэффициента K_{Γ} готовности КСА переработки информации;

максимизацию вероятности $p_{\text{с}}(T)$ сохранности в заданном интервале времени T использования ИМ;

минимизацию суммарных эксплуатационных затрат $\Sigma_j c_j$ эргасистемы и др.

Основными задачами *восстановительного* резервирования ИМ являются [5]:

определение областей наиболее эффективного его использования при различных условиях эксплуатации КСА;

определение типа носителей информации для размещения восстановительного резерва;

выбор оптимальных методов и структур восстановления потерянной информации;

выбор оптимальных стратегий резервирования с учетом возможности восстановления разрушенных ИМ.

Основными задачами *долговременного* резервирования ИМ являются [5]:

определение (расчет) рационального (необходимого) числа копий и (или) предысторий ИМ, обеспечива-

ющих заданный уровень вероятности сохранности ИМ-*оригинала* (основного ИМ);

создание и организация функционирования специализированных хранилищ и архивов МНИ (периодических проверок работоспособности, регенерации ИМ и др.);

определение оптимальных периодов создания долгосрочного восстановительного резерва.

Обоснованное комбинирование комплектов генерируемых копий, предысторий и дубликатов ИМ с учетом параметров режима (переходный, установившийся и др.) работы КСА позволяет реализовать рациональные (экономичные, оперативные и др.) ситуационные стратегии резервирования постоянных и текущих данных.

Общую математическую постановку *задачи обеспечения сохранности информации* (ОСИ) как задачи поиска оптимальной стратегии S_3 сохранения и подготовки ИМ (т. е. определения схем восстановления и регенерации ИМ, выбора методов резервирования ИМ, обнаружения и исправления ошибок и др.), которая обеспечивает максимизацию вероятности p_z успешного решения частной задачи эргасистемы при ограничении на среднее время $t'_ф$ функционирования КСА и суммарные потери и затраты $\Sigma_j c_j$, можно представить в виде:

$$K: p_z(S_3^*) = \max_{\{S3\}},$$
$$t'_ф(S_3^*) \le t'^{\,0}_ф, \quad (9)$$
$$\Sigma_j c_j(S_3^*) \le C_3^{\,0},$$
$$\Sigma_j c_j = c_1 + \check{c}_2 = \{s_1(t'_ф - \theta) + s_2(n)\} + \quad (10)$$
$$+ s_3(1 - p_z),$$

где c_1 — затраты, связанные с резервированием ИМ; $\check{c}_2$ — математическое ожидание потерь, которые несет эргасистема в результате разрушения основного ИМ M_0 и его копий; s_1 — стоимость единицы машинного времени; $s_2(n)$ — стоимость материального носителя ИМ, зависящая от количества n запоминающих устройств для хранения копий либо предысторий ИМ M_0; s_3 — потери эргасистемы в результате разрушения ИМ M_0 и его копий; θ — время решения частной задачи эргасистемы.

Кроме того, эффективность применения различных стратегий $S_3 \in \Delta_3$ ОСИ часто определяется также с использованием следующих *показателей готовности* КСА переработки информации различного типа [5]:

– готовность в установившемся режиме — относительное время полезной работы КСА на достаточно большом интервале времени:

$$K_Г = t'_ф/[t'_ф + (1 - p_z)t'_v], \quad (11)$$

где t'_v — среднее время восстановления КСА;

– готовность в заданном интервале — относительное время нахождения КСА в работоспособном состоянии на ограниченном интервале T времени функционирования:

$$K_Г = (T - T_v)/T, \quad (12)$$

где T_v — суммарные затраты времени на восстановление КСА в интервале $[0, T]$;

– мгновенная готовность — вероятность того, что в произвольный момент времени КСА работоспособен:

$$K_Г = 1 - Q(t), \quad (13)$$

где $Q(t)$ — вероятность того, что ИМ неработоспособен в момент времени t хранения;

– коэффициент эксплуатационной надёжности — вероятность решения задачи эргасистемы с учётом начального состояния КСА:

$$K_э = p_z K_Г; \quad (14)$$

– коэффициент полезной работы, определяемый как отношение времени полезной работы КСА к суммарному времени доступа к КСА при решении задачи:

$$K_п = \theta/t'_ф. \quad (15)$$

Таким образом, рассмотрена непротиворечивая совокупность *принципов* КЗИ в эргасистеме, следование которым обеспечивает, как показала практика, необходимый уровень защищённости перерабатываемой информации от основных разрушающих факторов, ошибок переработки, несанкционированного доступа и использования на основе применения соответствующих *методов* КЗИ.

Литература

1. Анин Б. Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2016. 384 с.
2. Барсуков В. С., Водолазний В. В. Современные технологии безопасности. М. : Нолидж, 2014. 496 с.
3. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М. : Горячая линия — Телеком, 2010. 272 с.
4. Дейт К. Дж. Введение в системы баз данных. М. : Изд. дом «Вильямс», 2005. 1328 с. ISBN 5-8459-0788-8.
5. Кульба В. В., Ковалевский С. С., Шелков А. Б. Достоверность и сохранность информации в АСУ. М. : Синтег, 2004. 496 с.
6. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : Росс. гос. ун-т правосудия, 2016. 316 с.
7. Ловцов Д. А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере. II. Качество информации // Правовая информатика. 2015. № 2. С. 53–61.
8. Ловцов Д. А. Информационная безопасность и нетрадиционные угрозы // Федеральный справочник. Т. 8. Оборонно-промышленный комплекс России. М. : Центр стратег. исследований, 2013. С. 507—512.
9. Ловцов Д. А. Информационная теория эргасистем : тезаурус. М. : Наука, 2005. 248 с.
10. Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1–7.

11. Ловцов Д. А., Ермаков И. В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1–9.
12. Ловцов Д. А., Князев К. В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100–103; II. Качество информационно-математического обеспечения // Информация и космос. 2013. № 2. С. 95–100.
13. Ловцов Д. А., Терентьева Л. В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. 2020. Т. 73. № 7. С. 115–126. DOI: 10.17803/1729-5920.2020.164.7.115-126.
14. Монахов М. Ю., Монахов Ю. М., Полянский Д. А. Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах : монография. Владимир : Изд-во ВлГУ, 2015. 208 с. ISBN 978-5-9984-0634-8.
15. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М. : ДМК, 2017. 448 с.
16. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50–58. DOI 10.21681/1994-1404-2018-4-50-58.

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, профессор кафедры автоматизированных систем управления Филиала Военной академии им. Петра Великого, г. Серпухов, Московская область, Российская Федерация.*
E-mail: tsimbalva@mail.ru

PRINCIPLES OF ENSURING INFORMATION SECURITY IN ERGASYSTEMS

Dmitrii Lovtsov, *Dr.Sc. (Technology), Professor, Meritorious Scientist of the Russian Federation, Deputy Director for Research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Russian Federation, Moscow.*
E-mail: *dal-1206@mail.ru*

Keywords: *ergasystem, information security, reliability, confidentiality, integrity, principles of ensuring, processing errors, destructive factors, unauthorised access and use, ways to protect information, mathematical structures.*

Abstract.
Purpose of the work: improving the scientific and methodological basis of the theory of information security in ergasystems.
Methods used: system analysis, pragmatic classification and mathematical modelling of the basic specific tasks of ensuring information security in ergasystems.
Results obtained: a justification is given for a consistent set of principles for information control and protection from processing errors, destructive factors, and unauthorised access and use, for a pragmatic classification of information processing errors, destructive factors, sources of potential information leaks as well as corresponding ways to protect information, mathematical structures for models of problems ensuring information reliability, confidentiality and integrity in ergasystems are defined, proofs for assertions on raising information reliability, on perfect semantic concealment and on energy concealment of dynamic information are given.
The obtained results are the conceptual basis for creating appropriate efficient information and mathematical support for control and protection of information in ergasystems.

References

1. Anin B. Iu. Zashchita komp'iuternoi informatsii. SPb. : BKhV-Sankt-Peterburg, 2016, 384 pp.
2. Barsukov V. S., Vodolaznii V. V. Sovremennye tekhnologii bezopasnosti. M. : Nolidzh, 2014, 496 pp.
3. Vorona V. A., Tikhonov V. A. Sistemy kontrolia i upravleniia dostupom. M. : Goriachaia liniia – Telekom, 2010, 272 pp.
4. Deit K. Dzh. Vvedenie v sistemy baz dannykh. M. : Izd. dom "Vil'iams", 2005, 1328 pp. ISBN 5-8459-0788-8.
5. Kul'ba V. V., Kovalevskii S. S., Shelkov A. B. Dostovernost' i sokhrannost' informatsii v ASU. M. : Sinteg, 2004, 496 pp.
6. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : Ross. gos. un-t pravosudiia, 2016, 316 pp.

7. Lovtsov D. A. Lingvisticheskoe obespechenie pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. II. Kachestvo informatsii. Pravovaia informatika, 2015, No. 2, pp. 53—61.
8. Lovtsov D. A. Informatsionnaia bezopasnost' i netraditsionnye ugrozy, Federal'nyi spravochnik. T. 8. Oboronno-promyshlennyi kompleks Rossii. M. : Tsentr strateg. issledovanii, 2013, pp. 507—512.
9. Lovtsov D. A. Informatsionnaia teoriia ergasistem : tezaurus. M. : Nauka, 2005, 248 pp.
10. Lovtsov D. A., Ermakov I. V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme, NTI. Ser. 2. Inform. protsessy i sistemy, 2005, No. 2, pp. 1-7.
11. Lovtsov D. A., Ermakov I. V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam, NTI. Ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1-9.
12. Lovtsov D. A., Kniazev K. V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100-103; II. Kachestvo informatsionno-matematicheskogo obespecheniia. Informatsiia i kosmos, 2013, No. 2, pp. 95-100.
13. Lovtsov D. A., Terent'eva L. V. Pravovoe regulirovanie mezhdunarodnykh kommercheskikh elektronnykh kontraktov. Tekhnologicheskie i pravovye aspekty elektronnoi podpisi. Lex russica, 2020, t. 73, No. 7, pp. 115-126. DOI: 10.17803/1729-5920.2020.164.7.115-126 .
14. Monakhov M. Iu., Monakhov Iu. M., Polianskii D. A. Modeli obespecheniia dostovernosti i dostupnosti informatsii v informatsionno-telekommunikatsionnykh sistemakh : monografiia. Vladimir : Izd-vo VlGU, 2015, 208 pp. ISBN 978-5-9984-0634-8.
15. Petrov A. A. Komp'iuternaia bezopasnost'. Kriptograficheskie metody zashchity. M. : DMK, 2017, 448 pp.
16. Fedoseev S. V. Primenenie sovremennykh tekhnologii bol'shikh dannykh v pravovoi sfere. Pravovaia informatika, 2018, No. 4, pp. 50-58. DOI 10.21681/1994-1404-2018-4-50-58 .