МЕТОДЫ И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ЭРГАСИСТЕМАХ

Ловцов Д.А.*

Ключевые слова*: эргасистема, защищенность информации, достоверность, конфиденциальность, сохранность, методы обеспечения, аппаратно-программные процедуры, информационно-распределительная сеть, прагматическая классификация, показатели, критерии, подсистема контроля и защиты информации, организационно-функциональные принципы.*

Аннотация.

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

Методы: системный анализ, формализация сложной задачи, прагматическая классификация и распределение основных методов и аппаратно-программных процедур обеспечения защищенности информации в эргасистемах.

Результаты: определена математическая структура комплексной задачи обеспечения защищенности информации в эргасистемах; определена логическая последовательность методологических этапов разработки подсистемы контроля и защиты информации на основе прагматических организационно-функциональных принципов; обоснована непротиворечивая совокупность методов контроля и защиты информации от ошибок переработки, от разрушающих факторов и от несанкционированного доступа и использования; обоснована прагматическая классификация основных методов и распределение целесообразных сетевых аппаратно-программных процедур обеспечения защищенности информации в эргасистемах.

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

DOI: 10.21681/1994-1404-2021-3-34-49

Введение

С учетом обоснованной предметно-логической декомпозиции качества информации [4, 6, 7] решение *комплексной научной проблемы* обеспечения защищенности информации (ОЗИ) в эргасистемах возможно на основе *специальной методологии* контроля и защиты информации (КЗИ), определяющей взаимосвязь трех соответствующих научно-технических проблем: обеспечения *достоверности* (помехоустойчивости, помехозащищенности), *конфиденциальности* (скрытности, доступности, имитостойкости) и *сохранности* (целостности, готовности) информации, отдельных свойств информации и подсистемы КЗИ, основных показателей и критериев оптимизации КЗИ и представляющей собой:

учение (совокупность теоретических положений) о принципах и структурах подсистемы КЗИ, логической организации (технологии) КЗИ, системе способов и методик (методов и показателей) КЗИ, комплексе средств (видов обеспечений) КЗИ;

инструмент (совокупность технических решений), с помощью которого практически решается триединый комплекс научно-технических проблем КЗИ обеспечения достоверности, конфиденциальности и сохранности информации в существующих и перспективных эргасистемах.

Степень обеспечения *защищенности* информации в эргасистеме определяется, таким образом, состоянием решения проблем обеспечения достоверности, конфиденциальности и сохранности информации (контрольно-измерительной, командно-программной, технологической и др. [6]).

Формализация и анализ комплексной задачи обеспечения защищенности информации в эргасистемах

Обеспечение *достоверности* информации заключается в достижении требуемого уровня достоверно-

* ***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

сти путем внедрения методов контроля дестабилизирующих факторов (ДФ) и защиты информации на всех стадиях ее *переработки*[1], повышением надежности комплекса средств автоматизации (КСА) эргасистемы (включая комплексы технических и программных средств — КТС, КПС), административно-организационными мерами (моральным и материальным стимулированием, направленным на снижение числа ошибок, улучшением условий труда персонала, организацией селективного доступа и др.) [6, 7]. Критерии оптимальности при этом, как правило[2] [3] — минимизация:

вероятности (q_1) искажения единичного массива информации (ЕМИ);

суммарного среднего времени $(\Sigma_j t'_j)$ на обработку, контроль и исправление информационного массива (ИМ);

суммарных потерь с учетом затрат $(\Sigma_j c_j)$ на разработку и функционирование структур контроля, исправление ошибок и потери в эргасистеме при использовании недостоверной информации;

времени переработки ИМ и материальных затрат при ограничении на достоверность и др.,

а также — *максимизация* достоверности (D) переработки информации как некоторой функции вероятности (q_1) ошибки.

Обеспечение *конфиденциальности* информации (ОКИ) заключается в обеспечении требуемого уровня конфиденциальности и секретности ИМ путем дополнительного преобразования (семантического, операторного, криптографического, псевдослучайного, организационно-диалогового и др.) *привилегированной* информации, контроля полномочий программно-технических средств, ресурсов эргасистемы и лиц (операторов, персонала, пользователей и др.), взаимодействующих со средствами автоматизации, и разграничения доступа к ИМ. Прагматические критерии оптимальности[3] — *минимизация*:

вероятности (p_o) преодоления («взлома») защиты;

вероятности (p_w) определения пароля значности W по его отображениям;

суммарных $(\Sigma_j c_j)$ затрат (интеллектуальных, финансовых, материальных, временных и др.) на разработку и эксплуатацию подсистемы КЗИ при ограничениях на вероятность $(p_н)$ несанкционированного доступа (НСД);

суммарных $(\Sigma_i r_i + \Sigma_j c_j)$ потерь от «взлома» защиты и затрат на разработку и эксплуатацию соответствующих элементов подсистемы КЗИ и др.,

а также — максимизация ожидаемого безопасного времени $(\check{T}_o)$ до «взлома» подсистемы защиты.

Обеспечение *сохранности* информации (ОСИ) заключается в обеспечении необходимого уровня сохранности ИМ путем введения специальной организации хранения и подготовки, регенерации и восстановления ИМ, использования дополнительных ресурсов для их резервирования, что позволяет значительно уменьшить влияние разрушающих факторов на эффективность функционирования эргасистем в целом. Основные критерии оптимальности[4] [3] — *максимизация*:

вероятности (p_z) успешного решения определенной частной задачи эргасистемы при наличии соответствующих ИМ, их дубликатов, копий и (или) предысторий;

вероятности (p_t) сохранности ИМ за фиксированный интервал t времени их эксплуатации;

вероятности (p_v) восстановления ИМ и др.,

а также — *минимизация*:

среднего времени (t'_z) решения задачи эргасистемы;

среднего времени (t'_v) восстановления ИМ;

стоимостных затрат $(\Sigma_j c_j)$ на дополнительные носители информации для размещения резервных ИМ, потерь от разрушения ИМ и др.

Соответствующую общую математическую постановку задачи обеспечения защищенности информации в эргасистеме с учетом расширенной концепции [4] можно представить[5] в виде композиции математических формулировок частных задач обеспечения достоверности, конфиденциальности и сохранности ИМ соответственно:

$$K\colon F\{\lambda_k, D(S^*), \check{T}_o(S^*), p_z(S^*)\} = \max_{\{S\}}, \qquad (1)$$

$$\Sigma_j t'_j(S^*) \le T^0, \Sigma_i c_{1i}(S^*) \le C_1^{\,0}, j=1,\ldots,J;\ i=1,\ldots,I_1;$$
$$p_w(S^*) \le p_w^{\,0}, \Sigma_i c_{2i}(S^*) \le C_2^{\,0}, w=1,\ldots,W;\ i=1,\ldots,I_2;$$
$$t'_z(S^*) \le t_z^{\,0}, \Sigma_i c_{3i}(S^*) \le C_3^{\,0}, z=1,\ldots,Z;\ i=1,\ldots,I_3,$$

$$S = < S_1, S_2, S_3 >;\ S \in \Delta = \Delta_1 \times \Delta_2 \times \Delta_3$$
$$S_1 = < G, p_i = 1 - q_i, f_j = 1 - e_j, \tau_i, x_i, \vartheta_j, y_j, t_j, z_j, I, J >;$$
$$S_2 = < X, K^0, E, A(R), T, w+r, V >;$$
$$S_3 = < K, \tau, \Pi, N, p, \theta >;$$
$$\lambda_k \ge 0;\ \Sigma_k \lambda_k = 1,$$

где

Δ — множество допустимых решений-троек: структур S_1 переработки информации, наборов S_2 атрибутов доступа к ресурсам эргасистемы, стратегий S_3 сохранения и подготовки ИМ; λ_k, k =1, 2, 3 — весовые коэффициенты;

D — вероятность достоверной переработки ЕМИ в эргасистеме; $\check{T}_o$ — ожидаемое безопасное время работы КСА (время до раскрытия пароля (ключа) доступа); p_z — вероятность успешного решения функциональной задачи эргасистемы;

T^0 — директивное время переработки (обработки, контроля ДФ и исправления ошибок) информации; $C_1^{\,0}$ — заданный материальный ресурс на обработку,

[1] Ловцов Д. А. Защита информации от искажения при переработке // Информатика и образование. 1996. № 3. С. 84—89.

[2] 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.

[3] Там же.

[4] Там же.

[5] Там же.

контроль и исправление ошибочного ЕМИ; t'_z — среднее время функционирования КСА при решении частной задачи эргасистемы; p_w — вероятность НСД (определения пароля (ключа) по его отображениям);

$G = (A, B)$ — ориентированный граф-модель технологического процесса переработки информации (ТППИ) с множеством A, отображающих заданное множество задач переработки информации (ЗПИ), и множеством дуг[6] $B \subseteq A \times A$; p_i, $i = 1,\ldots,I$ — вероятность правильной обработки ЕМИ на i-м этапе ТППИ и, в частности, того, что ИМ-оригинал M_0 не разрушится за единичный интервал времени $t = 1$ при его обновлении; q_i — вероятность искажения ЕМИ; τ_i — время обработки ЕМИ (создания одной копии ИМ M_0); x_i — затраты на обработку ЕМИ; f_j, $j = 1,\ldots,J$ — вероятность обнаружения ДФ (ошибки) в ЕМИ на j-м этапе контроля; e_j — вероятность пропуска ДФ (ошибки); ϑ_j — время контроля ЕМИ; y_j — затраты на контроль ЕМИ; t_j — время исправления ЕМИ на j-м этапе контроля; z_j — затраты на исправление ошибочного ЕМИ; K — количество копий ИМ M_0; Π — количество предысторий ИМ M_0; $N = 1,\ldots,8$ — номер схемы восстановления ИМ;

$X = \{X_i\}$, $i = 1,\ldots,n$ — множество индивидуальных паролей (имен, алгоритмов, вопросов и др.) $X_i = \{x_{ij}\}$, $j = 1,\ldots,w_i$ n объектов эргасистемы; $E = \{E_i\}$, $i = 1,\ldots,n$ — множество соответствующих эталонных паролей, преобразованных [10] с целью защиты по соответствующему ключу $k_i \in K^0$ и хранящихся в специальной памяти эргасистемы; $A(R) = \{A_l(R_l)\}$, $l=1,\ldots,L$ — множество алфавитов различного размера R_l парольных символов $x_{ij} \in A_l(R_l)$; $T = < t_и, t_x, t_о, t_п, t_з >$ — определенное значение длительности цикла доступа, включающей 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; f — заданное значение числа разрешенных попыток доступа; $w+r$ — значность передаваемого сообщения (включая w символов пароля-стринга и r символов (служебных) идентификатора) при попытке получить доступ к ресурсам эргасистемы; V — скорость передачи данных (телеграфирования, если $A_0 = < 0,1 >$) в линии связи, *смв/с* (*бод*);

$\Sigma_i c_{2i} = c_{21} + \check{c}_{22} = c_{21} + g_1(1 - p_w)$ — суммарные затраты и потери эргасистемы на обеспечение конфиденциальности ИМ; c_{21} — затраты, связанные с разработкой и эксплуатацией элементов контроля и разграничения доступа; $\check{c}_{22}$ — математическое ожидание потерь, которые несет эргасистема в результате раскрытия привилегированной информации; g_1 — потери эргасистемы от несанкционированного использования одного ИМ;

$\Sigma_i c_{3i} = c_{31} + \check{c}_{32} = [g_2(t'_z - \theta) + g_3] + g_4(1 - p_z)$ — суммарные затраты и потери эргасистемы на обеспечение сохранности ИМ; c_{31} — затраты, связанные с резервированием ИМ; $\check{c}_{32}$ — математическое ожидание потерь, которые несет эргасистема в результате разрушения ИМ-оригинала M_0 и его копий; g_2 — стоимость единицы машинного времени; $g_3(L)$ — стоимость материального носителя ИМ, зависящая от количества L запоминающих устройств для хранения копий или предысторий ИМ-оригинала M_0; g_4 — потери эргасистемы в результате разрушения ИМ M_0 и его копий; θ — время решения частной задачи эргасистемы.

Совместное решение конкретных частных задач обеспечения *достоверности* (т. е. непосредственного назначения узлов обработки, определения этапов контроля и исправления обнаруженных ошибок, выбора методов обнаружения и исправления ошибок и др.), *конфиденциальности* (т. е. определения атрибутов и длительности цикла доступа, выбора методов контроля и разграничения доступа и др.) ИМ и *сохранности* (т. е. определения схем восстановления и регенерации ИМ, выбора методов резервирования ИМ, обнаружения и исправления ошибок и др.) с использованием рассмотренных в задаче (1) показателей эффективности и качества, а также известного математического аппарата [3, 5, 9, 10, 16, 19] позволит обеспечить требуемый уровень *защищенности* информации в реальной эргасистеме.

Последовательность разработки обобщенной подсистемы КЗИ (рис. 1) в эргасистеме включает ряд этапов оценивания, анализа и обоснования комплекса *средств* и *протоколов* (регламентов и процедур) КЗИ с учетом специфики трех основных научно-технических проблем ОЗИ.

При этом очевидно, что требуемый уровень защищенности ИМ в эргасистеме определяется соответствием между ценностью используемой информации и теми затратами (снижением производительности КСА, дополнительным расходом оперативной памяти КСА и др.), которые необходимы для его достижения. Поэтому разработчику нужен обоснованный показатель экономической эффективности, связывающий требуемый (заданный) уровень защиты и необходимые затраты на ее реализацию.

Можно, например, использовать коэффициент[7] $C_р$ накладных расходов, связанных с функционированием подсистемы КЗИ:

$$C_р = \{\Sigma_k \Sigma_j F(a_k, r_j)\}/\{\Sigma_i \Sigma_j F(m_i, r_j)\}, \quad (2)$$

где $R = \{r_j\}$, $j=1,\ldots,J$ — кортеж ресурсов КСА; $M = \{m_i\}$, $i=1,\ldots,I$ — кортеж системных процедур КСА; $A = \{a_k\}$, $k=1,\ldots,K$ — кортеж системных процедур подсистемы КЗИ $(A \subseteq M)$; F — показатель

[6] Ловцов Д. А. Планирование и прогнозирование процессов обмена привилегированной информацией в сети АСУ // Зарубежная радиоэлектроника. 1996. № 2. С. 7—64; Ситуационное планирование процесса переработки измерительной информации в сети АСУ // Изв. РАН. Теория и системы управления. 1995. № 5. С. 239—247.

[7] Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 246 с.

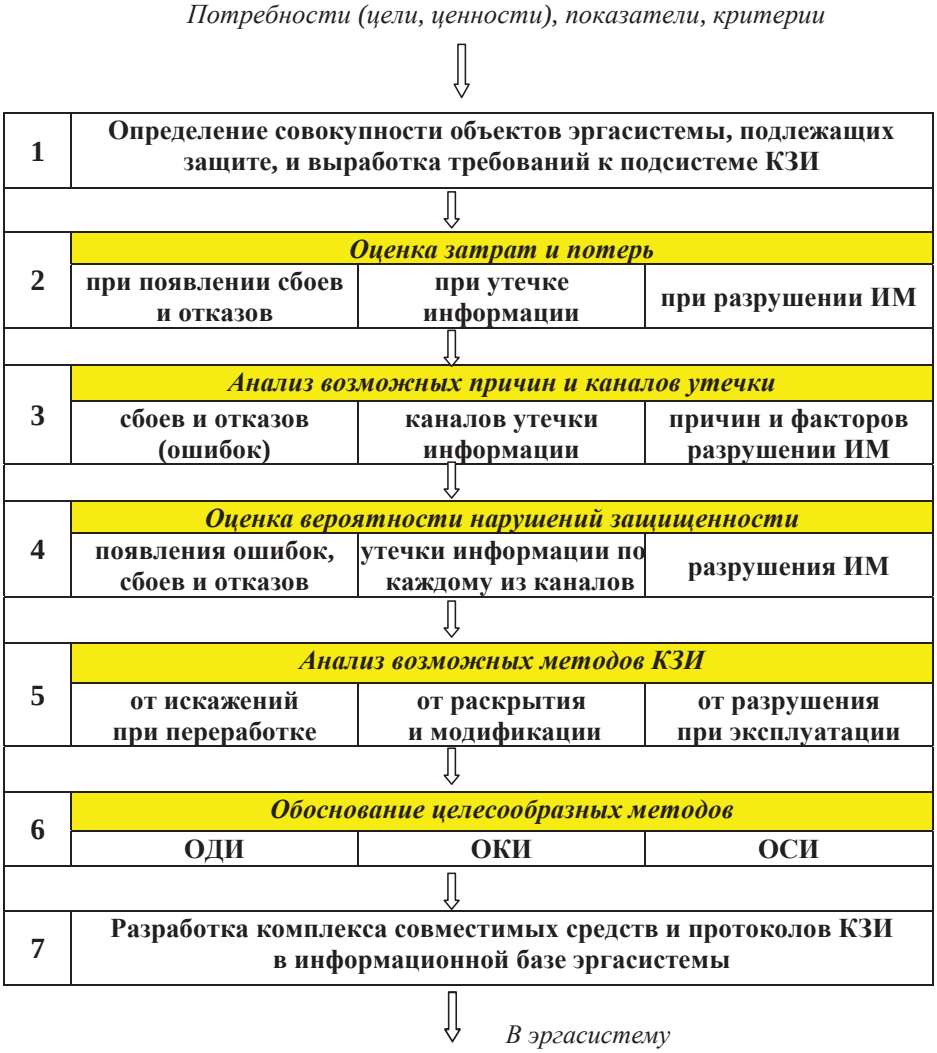

Рис. 1. Логическая последовательность методологических этапов разработки подсистемы контроля и защиты информации

(количественная мера) использования ресурса r_j процедурой m_i или a_k.

При наличии зависимостей типа (2) разработчик может определить процедуры КЗИ и их объемы, которые должны быть использованы в КСА, при этом экономические методы КЗИ дадут накладные расходы, приближающиеся к нулю.

В общем случае применяемая *мера противодействия* (КЗИ) с экономической точки зрения будет приемлема, если эффективность защиты с ее помощью, выраженная через снижение вероятного экономического ущерба, превышает затраты на ее реализацию — так называемый *принцип разумной достаточности*.

Опыт разработки и создания реальных обобщенных подсистем КЗИ в настоящее время еще недостаточен. Вместе с тем известен ряд прагматических *организационно-функциональных принципов*[8] [5, 9] построения подсистем КЗИ, учет которых позволяет уменьшить количество недостатков разрабатываемых подсистем в существующих эргасистемах:

ситуационность (обеспечивает учет сложившейся темпоральной стереотипной ситуации и текущих требований обладателей информации при определении и установлении соответствующего уровня защищенности информации);

целевая эффективность (обеспечивает рациональность использования для защиты информации общесистемных средств и ресурсов);

«тотальность» контроля (обеспечивает всестороннюю проверку возможных традиционных и нетрадиционных каналов доступа к любому защищаемому объекту эргасистемы);

полнота контроля (обеспечивает всестороннюю проверку качества всех ИМ и полномочий любого обращения к любому защищаемому объекту эргасистемы);

простота протоколов КЗИ (обеспечивает отсутствие ошибок проектирования);

обособленность протоколов КЗИ (обеспечивает минимизацию количества объектов эргасистемы, использующих одинаковые параметры и характеристики любого протокола защиты);

[8] Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 246 с.;

Шураков В. В. Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1985. 224 с.

несекретность проектирования (обеспечивает выявление и исправление максимального числа «врожденных» недостатков, дефектов и уязвимостей подсистемы КЗИ за счет привлечения различных специалистов);

разделение полномочий (обеспечивает достаточную гибкость и надежность подсистемы КЗИ путем физического разнесения нескольких используемых ключей для открытия процедуры защиты);

минимальность полномочий (обеспечивает использование объектами эргасистемы только тех ИМ, которые необходимы им для выполнения своих функций);

преобладание запретов над разрешениями (обеспечивает доступ и использование ИМ только в случае строгого выполнения определенных условий);

психологическая привлекательность (обеспечивает уменьшение количества попыток лицами, взаимодействующими с комплексом (ЛВК) средств автоматизации, искать обходные пути для доступа к ИМ и их использования).

Методы обеспечения достоверности информации

Использование методов обеспечения достоверности информации (ОДИ) требует введения в структуры переработки ИМ информационной, временной или структурной избыточности.

Структурная избыточность характеризуется введением в состав эргасистем дополнительных элементов (резервирование ИМ, реализация одной функции различными процедурами, схемный контроль в КТС и др.). *Временная* избыточность связана с возможностью неоднократного повторения определенного контролируемого этапа (фазы) переработки информации. *Информационная* избыточность характеризуется введением дополнительных информационных разрядов в используемые ИМ и дополнительных операций в процедуры переработки ИМ, имеющих математическую или логическую связь с алгоритмом переработки, обеспечивающих в результате применения выявление и исправление ошибок определенного типа. Наряду с такой информационной избыточностью, называемой *специальной*, используется и *естественная*, характеризуемая наличием ИМ, логическая связь между которыми позволяет судить об их достоверности.

Известные[9] методы обеспечения (повышения) достоверности перерабатываемой информации в эргасистеме можно разделить (по виду реализации) на две основные группы (рис. 2): организационные (системные и административные); технические (программные и аппаратные).

Организационные методы повышения достоверности состоят в создании и использовании рациональной технологии процесса переработки информации, предусматривающей профилактические меры по снижению доли ошибок переработки до определенного допустимого уровня.

Методы обеспечения надежности (см. *рис.* 2) КСА включают две большие группы методов обеспечения надежности КТС и КПС.

Надежность КСА — свойство КСА выполнять заданные функции, сохраняя во времени значения установленных эксплуатационных показателей в заданных пределах, соответствующих заданным режимам и условиям использования, технического обслуживания, ремонта, хранения и транспортирования. Надежность КТС определяется в основном *случайными* сбоями и отказами, а *надежность* КПС — наличием, как правило, систематических ошибок, допущенных при его разработке. При этом отказ (сбой) технического средства зависит от времени [4] и не зависит от перерабатываемой информации, а программные ошибки являются функцией от текущей входной информации и текущего состояния эргасистемы.

В связи с этим для ОДИ в эргасистеме используются общие типовые методы [14] обеспечения надежности аппаратуры, целью которых является поддержание характеристик КТС эргасистемы в заданных пределах.

Достижения в области повышения надежности КПС в настоящее время гораздо менее ощутимы, чем в надежности КТС, ввиду большой физической сложности КПС, зависимости его от предметной области применения, примитивности «комплектующих» стандартных блоков (операторов языка, сегментов старых программ и др.) с точки зрения конечного результата (единого целого).

Основными методами повышения надежности КПС являются методы контроля его качества, включающего три перекрывающиеся стадии: *отладку, тестирование* (с локализацией и исправлением ошибок) и формальное *доказательство* корректности КПС (соответствия программных компонентов формальным требованиям и логическим утверждениям технического проекта или задания).

Тестирование КПС включает проведение следующих работ[10]:

проектирование набора тестовых комбинаций на основе анализа внешних спецификаций и компонентов КПС, предусматривающее разработку проверочных тестов для логической схемы компонентов (модулей) КПС на чувствительность к различным входным характеристикам; каждого условия и варианта данных; границ всех заданных интервалов на входе и выходе; границ обрабатываемых ИМ для неверных условий и др.;

написание и проверка программ-тестов, предназначенных для тестирования единичных модулей, функционального тестирования (не в рабочих условиях), системного тестирования (в экстремальных режимах функционирования в рабочих или эксплуата-

[9] Мельников Ю. Н. Достоверность информации в сложных системах. М. : Сов. радио, 1974. 192 с.

[10] Шураков В. В. Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1985. 224 с.

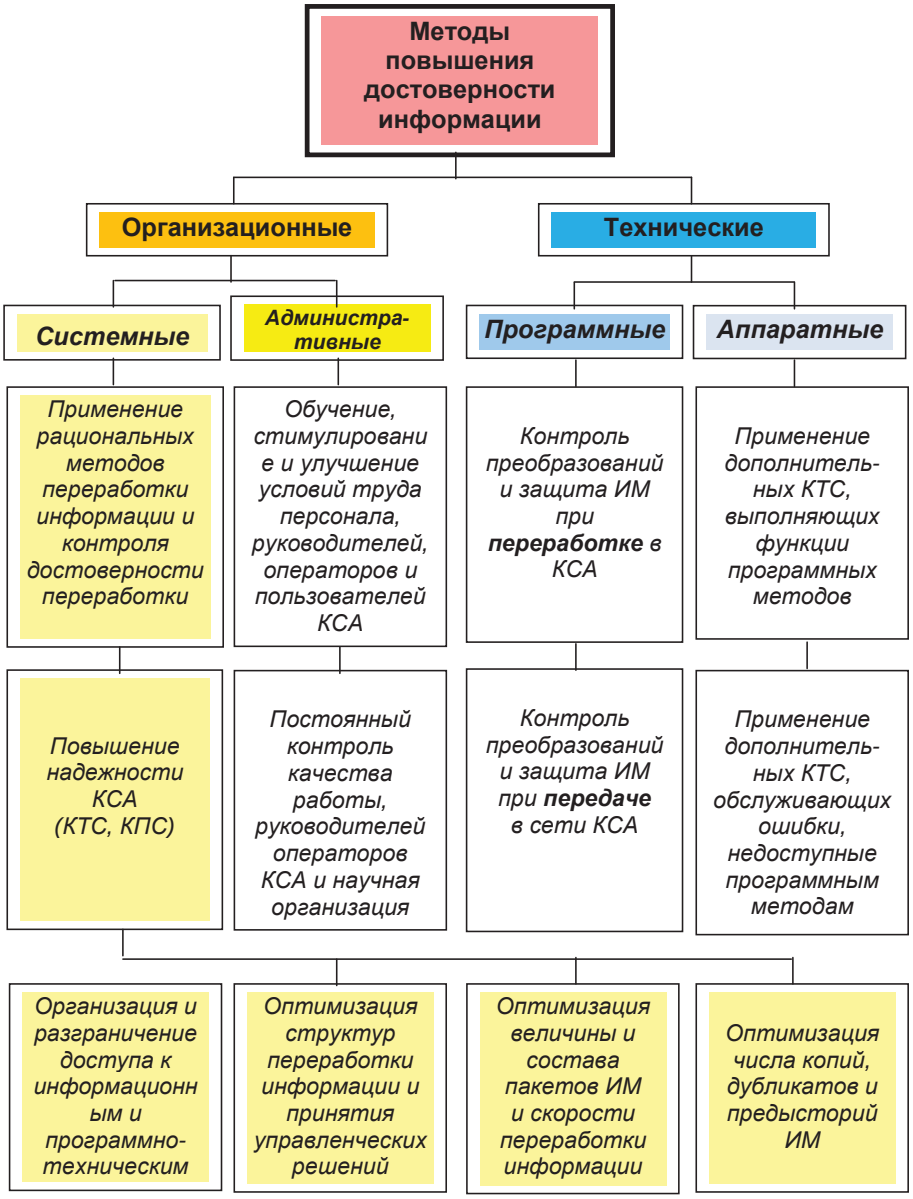

Рис. 2. Общая классификация методов повышения достоверности информации в эргасистемах

ционных условиях), приемо-сдаточного тестирования (в эксплуатационных условиях);

выполнение тестирования (модулей КПС, функционального, системного, приемо-сдаточного и установочного).

Технические методы повышения достоверности перерабатываемой в эргасистеме информации представляют собой совокупность программных и аппаратных методов контроля и выявления ошибок в исходных и получаемых ИМ, их локализации и исправления.

Программные методы включают методы контроля преобразований и защиты ИМ при переработке и методы КЗИ, передаваемой в подсистеме информационного обмена эргасистемы. Программные методы предусматривают дополнительные операции в процедурах переработки информации, которые имеют математическую или логическую связь с алгоритмом переработки информации (преобразования и передачи ИМ). Сравнение результатов этих дополнительных операций с результатами переработки информации дает возможность установить с определенной вероятностью наличие или отсутствие ошибок, а также исправить обнаруженную ошибку.

Аппаратные методы повышения достоверности выполняют практически те же функции, что и программные методы, кроме того, позволяют обнаруживать ошибки ближе к месту их возникновения, а также ошибки, недоступные для программных методов (например, перемежающиеся ошибки). Ими можно пользоваться для представления ЛВК более точной информации об искажениях, вызванных неисправностью КТС.

Сравнение программных и аппаратных методов повышения достоверности показывает, что при относительно сжатых сроках разработки эргасистемы максимальная (заданная) достоверность перерабатываемой информации достигается при использовании

комплекса организационных и программных методов повышения достоверности. Однако параллельно следует работать и над развитием аппаратных методов, новых КТС переработки ИМ, а также моделей и алгоритмов переработки информации и контроля ее достоверности. Анализ методов и определение оптимальной их комбинации, максимизирующей достоверность переработки информации, целесообразно проводить на основе аппарата математического программирования[11] с учетом ограничений на материальные и временные затраты при обеспечении заданного уровня достоверности.

Кроме того, выбор комбинации методов ОДИ определяется технологией переработки информации в эргасистеме, используемыми моделями возникновения ошибок и их взаимодействия, в результате анализа которых рассчитываются вероятности обнаружения и исправления ошибок для различных вариантов структур переработки информации и методов обеспечения требуемого уровня достоверности.

Методы обеспечения конфиденциальности информации

Множество методов ОКИ в эргасистеме можно разделить (по виду реализации) на две основные группы[12] [13, 18] (рис. 3):

организационные (80%), включая административные (50%), физические (22%), законодательные (8%);

технические (20%), включая аппаратные, программные, криптографические.

Административными методами в эргасистеме называется комплекс организационно-правовых мероприятий, регламентирующих (на основе нормативных правовых актов) процессы функционирования эргасистемы, использование ее КТС и информационно-программных ресурсов, а также взаимоотношения ЛВК и эргасистем с целью исключения возможности или существенного затруднения НСД к ИМ. Административные методы ОКИ играют большую роль в создании надежной подсистемы КЗИ от НСД и несанкционированного использования (НСИ), обеспечивая объединение всех организационно-технических средств в единое целое, поскольку возможности НСИ в значительной мере обусловливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью ЛВК и др. При помощи административных методов создается необходимая совокупность организационных, организационно-технических, организационно-правовых и др. мероприятий, охватывающая все структурные элементы эргасистемы на всех этапах ее жизненного цикла и приводящая к минимуму (исключающая) возможность утечки информации. Основными *мероприятиями* в такой совокупности являются следующие:

мероприятия при проектировании, строительстве и оборудовании объектов (центров, периферийных элементов и др.) эргасистем по исключению влияния стихийных бедствий, возможностей тайного проникновения в помещения, по обеспечению удобств для контроля прохода и перемещения людей и др.);

организация противопожарной службы;

подбор и подготовка персонала эргасистем (проверка принимаемых на работу, создание условий и стимулирование персонала, обучение правилам работы с привилегированной (закрытой и др.) информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.);

организация надежного пропускного режима;

организация хранения, выдачи и использования документов и носителей информации (определение соответствующих правил, маркировка, ведение журналов выдачи и использования и др.);

организация работы в дежурных сменах эргасистем (выделение ответственных за ОЗИ или создание специальной штатной службы, организация контроля за работой персонала, ведение журналов работы, уничтожение в установленном порядке производственных отходов и др.);

контроль внесения изменений в математическое и программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка всех изменений на удовлетворение требованиям ОКИ, документальное отображение изменений и др.);

организация подготовки и контроля работы ЛВК;

планирование мероприятий по ОКИ.

Физическими методами ОКИ в эргасистеме называется комплекс мер и мероприятий, предназначенных для создания физических препятствий (на основе применения различных специальных устройств и сооружений) для потенциальных нарушителей на пути в места, в которых можно иметь доступ к защищаемой информации. Они играют важную роль в комплексе мероприятий по ОКИ, затрудняя использование и прямых, и косвенных каналов утечки информации путем:

физической изоляции сооружений, в которых размещены КСА, от других сооружений;

ограждения территории объектов (элементов и каналов связи) эргасистем заборами (стенами) на расстояниях, достаточных для исключения эффективной регистрации электромагнитных излучений (ЭМИ);

контроля территорий объектов эргасистем;

создания контрольно-пропускных пунктов у входов в помещения объектов эргасистем для проверки ЛВК с точки зрения идентичности, аутентичности и наличия полномочий;

оборудования входных дверей специальными (кодовыми) замками, позволяющими регулировать доступ в помещения;

---

[11] Ловцов Д. А., Князев А. Г. Оптимизация структуры достоверной переработки информации // НТИ. Сер. 3. Информ. процессы и системы. 1998. № 10. С. 20—27.

[12] Там же. Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 246 с.

оборудование окон специальными средствами и материалами, не позволяющими осуществлять наблюдение за работой персонала и функционированием КТС;

оборудование дверей и створок шкафов аппаратуры специальными устройствами (механическими, электромеханическими, электронно-механическими и др.), препятствующими НСД;

организации системы охранной сигнализации.

Физические меры ОКИ должны быть предусмотрены для зон, откуда отправляют исходящие и где получают входящие документы, комнат программистов, полок в местах расположения вынесенных терминалов, погрузочных тележек, емкостей для транспортировки ИМ и др., т. е. там, где возможен ввод или вывод привилегированной информации.

Законодательные методы — это комплекс мер, определяемых законами страны, указами руководящих органов и соответствующими положениями, регламентирующими правила переработки и использования информации ограниченного доступа и распространения, а также ответственность за их нарушения, препятствуя тем самым НСИ [15].

Кроме того, для создания соответствующей законодательной защиты конфиденциальности информации в эргасистеме можно применять обычные положения об охране авторских прав, положение о выдаче лицензий, разрешений на снятие копий или сдачу в аренду и наложение требования о вручении в нераспечатанном виде. В качестве *дополнительных* технических мер можно использовать либо нанесение на носитель только объектного кода, либо переключение индивидуальных ИМ для прогона только на определенных центральных процессорах КСА (если их могут однозначно идентифицировать ИМ), либо включение нефункциональных (пустых) подпрограмм в ИМ ЛВК, обеспечивающих внесение искажений в случае неавторизованного использования и др.

Дополнительно к административным правилам часто используются *этические кодексы* поведения [8], определяющие профессиональные идеалы (этические соображения) и позволяющие повысить бдительность, внимательность и организованность персонала эргасистем и их информационно-распределительных сетей (ИРС).

Аппаратными (схемными) методами ОКИ называется комплекс технических мероприятий по разработке и использованию специальных схем и устройств КЗИ (электронных, электронно-механических, электронно-оптических и др.), встроенных конструктивно в серийные образцы технических средств эргасистем или самостоятельных (в составе КТС), позволяющих изолировать ЛВК друг от друга и от операционной системы КСА, обеспечивая при этом возможность эффективного контроля операций по переработке ИМ и уменьшая тем самым вероятность НСИ.

Основными методами аппаратного ОКИ в эргасистемах являются мероприятия по защите информационных массивов в КСА, т. е. в информационно-вычислительных комплексах (ИВК), комплексах командно-измерительных средств (ККИС), комплексах сбора и подготовки информации (КСПИ), комплексах отображения информации (КОИ), а также в каналах связи (КС) и передачи данных, в базах данных и знаний (БДЗ).

Аппаратные методы ОКИ широко применяются в современных эргасистемах, главным образом благодаря их надежности, однако исключительное использование данных методов нецелесообразно по экономическим соображениям (из-за высокой стоимости аппаратных средств и низкой их *адаптируемости* к изменяющимся условиям эксплуатации эргасистем). Состав, типы (общие, специфические или др.) и виды аппаратных методов и средств ОКИ определяются организационно-технической, функциональной и информационной структурами конкретных эргасистем. К настоящему времени разработано значительное число аппаратных средств различного назначения, при этом наибольшее распространение получают следующие[13] [16]:

специальные регистры для хранения реквизитов КЗИ (паролей, идентифицирующих кодов, грифов или уровней секретности и др.);

генераторы кодов для автоматического генерирования идентифицирующего кода устройства (терминала и др.) при включении его в работу и обращении к ресурсам эргасистемы или ИМ коллективного пользования;

устройства считывания кодов с перфокарт или магнитных карт, агрегируемые с замками включения технических средств в работу;

устройства измерения индивидуальных характеристик человека (голоса, узора папиллярных линий, длины пальцев и др.) с целью его идентификации [10];

схемы контроля границ адреса запоминающего устройства с целью определения законности обращения к заданному полю памяти;

схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных [14];

специальные биты секретности, значение которых определяет уровень секретности ИМ, хранимых в той части запоминающего устройства, которой принадлежат данные биты.

Вспомогательные аппаратные средства обеспечивают уничтожение использованных ИМ на магнитных носителях, сигнализируют о попытках несанкционированных действий и др. Особую группу аппаратных средств, получившую наибольшее распространение, составляют устройства преобразования информации.

Программными методами ОКИ (*рис*. 3) называется комплекс специальных алгоритмов и компонентов общего программного обеспечения эргасистем, предназначенных для выполнения функций контроля, разграничения доступа и исключения НСИ.

Программные методы являются наиболее распространенными методами ОКИ вследствие их универ-

[13] Там же.

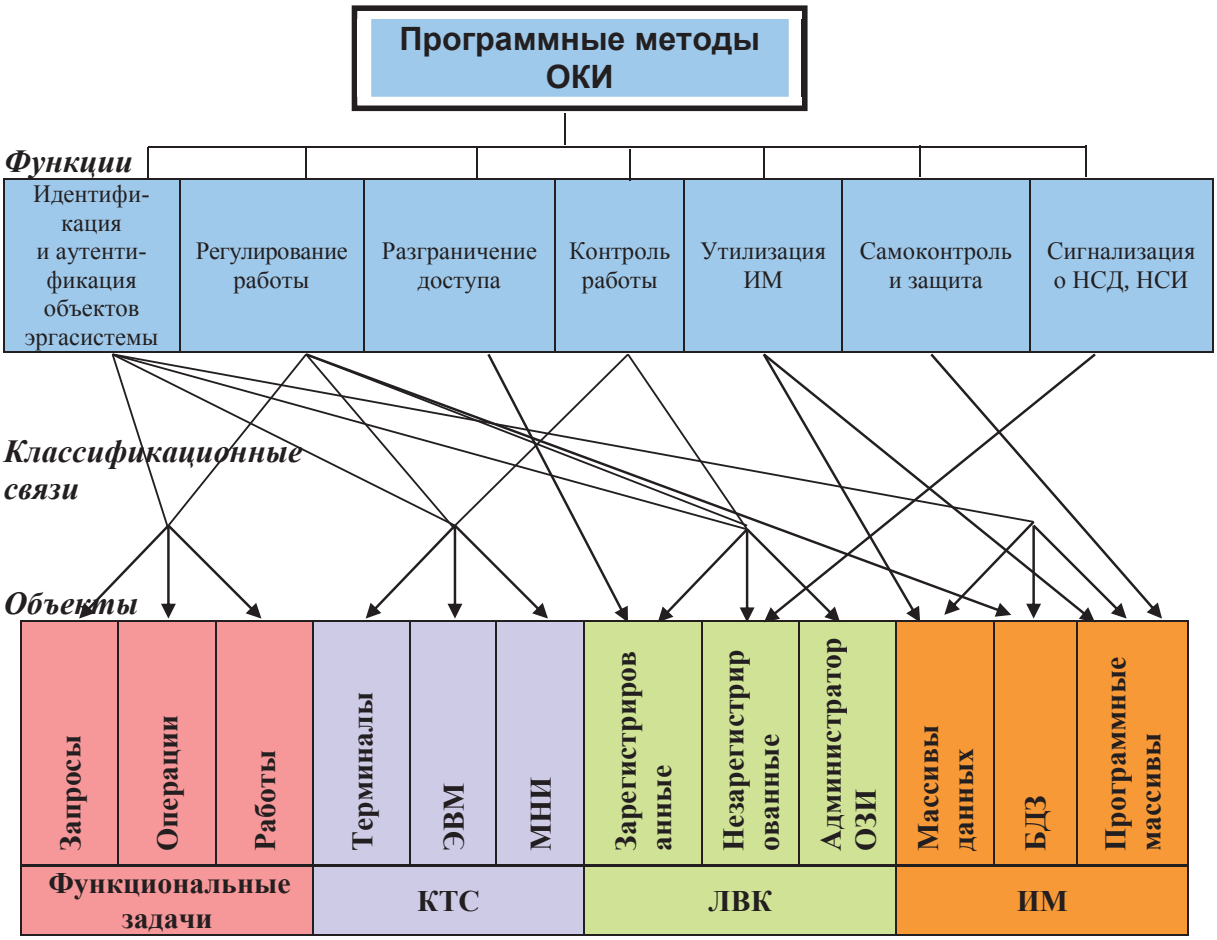

Рис. 3. Общая классификация программных методов обеспечения конфиденциальности информации в эргасистемах

сальности, гибкости, простоты реализации, возможности развития и адаптации к изменяющимся условиям эксплуатации эргасистем и др. Однако они имеют ряд *недостатков*, таких как расходование ресурса ЦП КСА на их функционирование, возможность несанкционированного изменения, невозможность их реализации там, где отсутствует процессор, и др. Программная защита, как правило, применяется там, где введение и использование других методов и средств КЗИ затруднено. По функциональному назначению множество существующих программных методов можно разделить на несколько групп (см. *рис.* 3).

Контроль и защита программных массивов осуществляется путем проверок по контрольным суммам, перезагрузки, организации точек входа, дублирования, криптографического закрытия, модульного диалога и др.

Вспомогательные программы КЗИ обеспечивают уничтожение остаточной информации на магнитных носителях, категорирование «грифованной» информации, формирование грифа секретности выдаваемых документов, имитацию работы с нарушителем для отвлечения его внимания и накопления сведений о характере запросов, ведение регистрационных журналов (для каждого запроса фиксируется выделяемое КСА время, ИМ, используемый терминал, суть запроса или задания, а также информация о том, был разрешен доступ или нет), общий контроль функционирования подсистемы ОКИ, программные проверки для КЗИ при схемных и программных сбоях и др. Особую группу, как и в случае с аппаратными методами, составляют программы преобразования (шифрования и кодирования) информации.

Криптографические методы ОКИ в эргасистемах — это комплекс процедур и алгоритмов преобразования информации, обеспечивающих скрытие смыслового содержания ИМ [1, 19] (*рис.* 4).

Криптографическое закрытие на основе шифрования и кодирования ИМ в эргасистемах исследуется в настоящее время по следующим основным *направлениям* [9, 11, 12]: выбор *рациональных* (надежных) систем и методов шифрования; обеспечение оптимального сочетания требований по *производительности* (быстроте передачи информации) и *криптостойкости* криптографических алгоритмов путем перехода к быстрым алгоритмам электронной подписи, основанным на принципиально других методах расчета (например, на теории графов вместо модульной арифметики); обоснование путей реализации систем шифрования в эргасистемах; разработка правил использования криптографических методов в процессе функционирования эргасистем; оценка эффективности криптографической защиты.

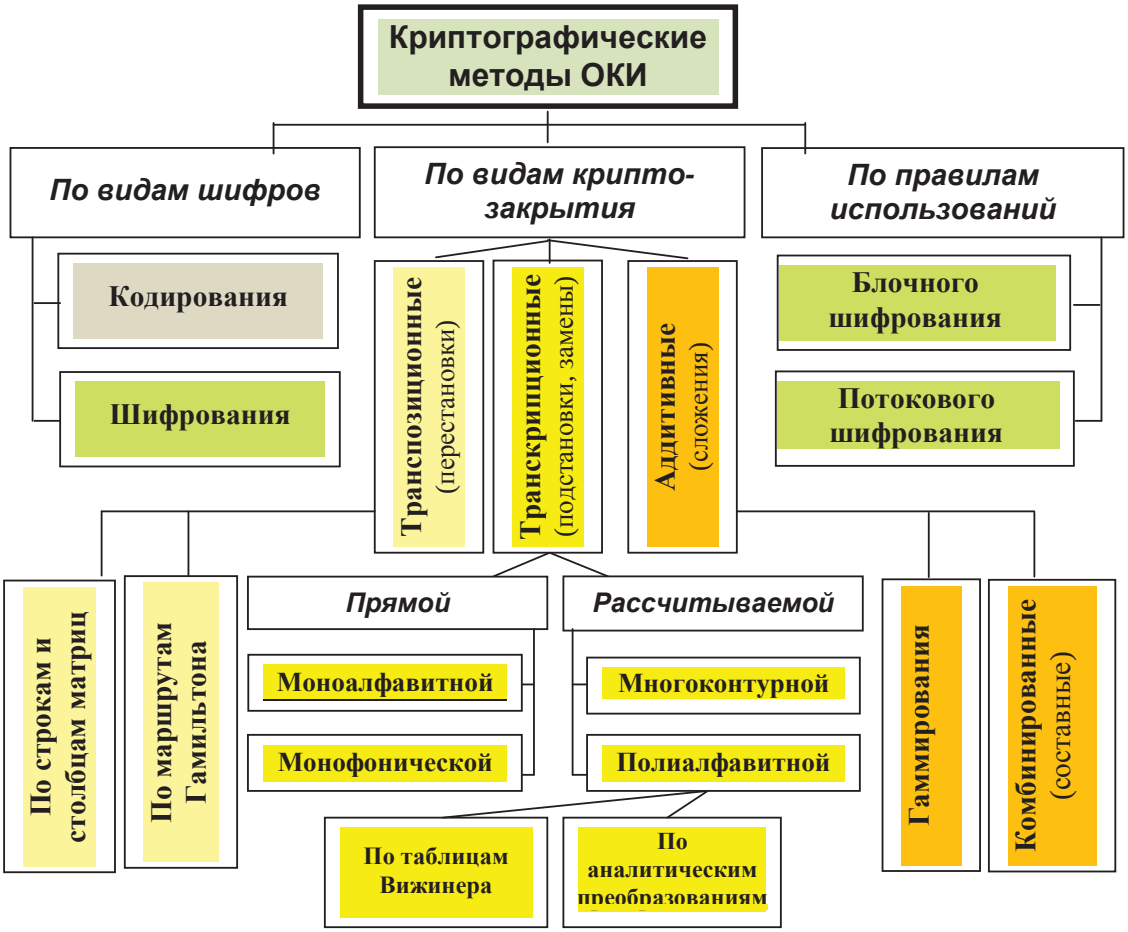

Рис. 4. Общая классификация криптографических методов обеспечения конфиденциальности информации в эргасистемах

Методы обеспечения сохранности информации

Методы обеспечения сохранности ИМ в эргасистеме относятся в основном к области организации и эксплуатации *внутримашинной информационной базы* [6] эргасистемы, реализованной на магнитных носителях, как правило, в виде комплекса функциональных баз данных и знаний (БДЗ).

Организация хранения и использования *статической* информации в БДЗ эргасистемы имеет свои специфические особенности [6], в частности, множество ИМ включает общие, групповые и индивидуальные (личные), что обусловливает необходимость создания гибкой защиты информации, учитывающей особенности использования различных ИМ. Для обеспечения гибкой защиты ИМ необходимо, чтобы система управления БДЗ (СУБД) допускала как частично совпадающие, так и даже противоположные друг другу требования по защите ИМ для различных ЛВК. При отсутствии единых представлений о структуре БДЗ отдельные ЛВК, не зная спецификаций защиты, установленных администратором, могут не получить доступа к данным. В СУБД, кроме стандартных атрибутов ИМ, учитываются и семантические отношения между ними. Эффективность защиты ИМ существенно зависит от способности СУБД обрабатывать отношения. Последние чувствительны к контексту, в котором связанные ИМ появляются, поэтому для организации защиты ИМ необходимо, чтобы СУБД умела их распознавать.

Известные[14] [3] методы повышения сохранности накапливаемой в БДЗ информации можно разделить (*по виду реализации*) на организационные (системные и административные) и технические (программные и аппаратные).

Организационные методы повышения сохранности (рис. 5) состоят в создании и использовании рациональной технологии эксплуатации (хранения и применения) ИМ, предусматривающей профилактические меры по снижению доли искажений ИМ до определенного допустимого уровня и обеспечению своевременного предоставления необходимых аутентичных ИМ для автоматизированного решения задач эргасистемы.

Административные методы научной организации труда (НОТ) персонала эргасистем предусматривают реализацию ряда *принципов*, обеспечивающих уменьшение возможностей нарушения (со стороны персонала) требований сохранности ИМ, основные из которых:

[14] Мамиконов А. Г., Кульба В. В., Шелков А. Б. Достоверность, защита и резервирование информации в АСУ. М. : Энергоиздат, 1986. 304 с.

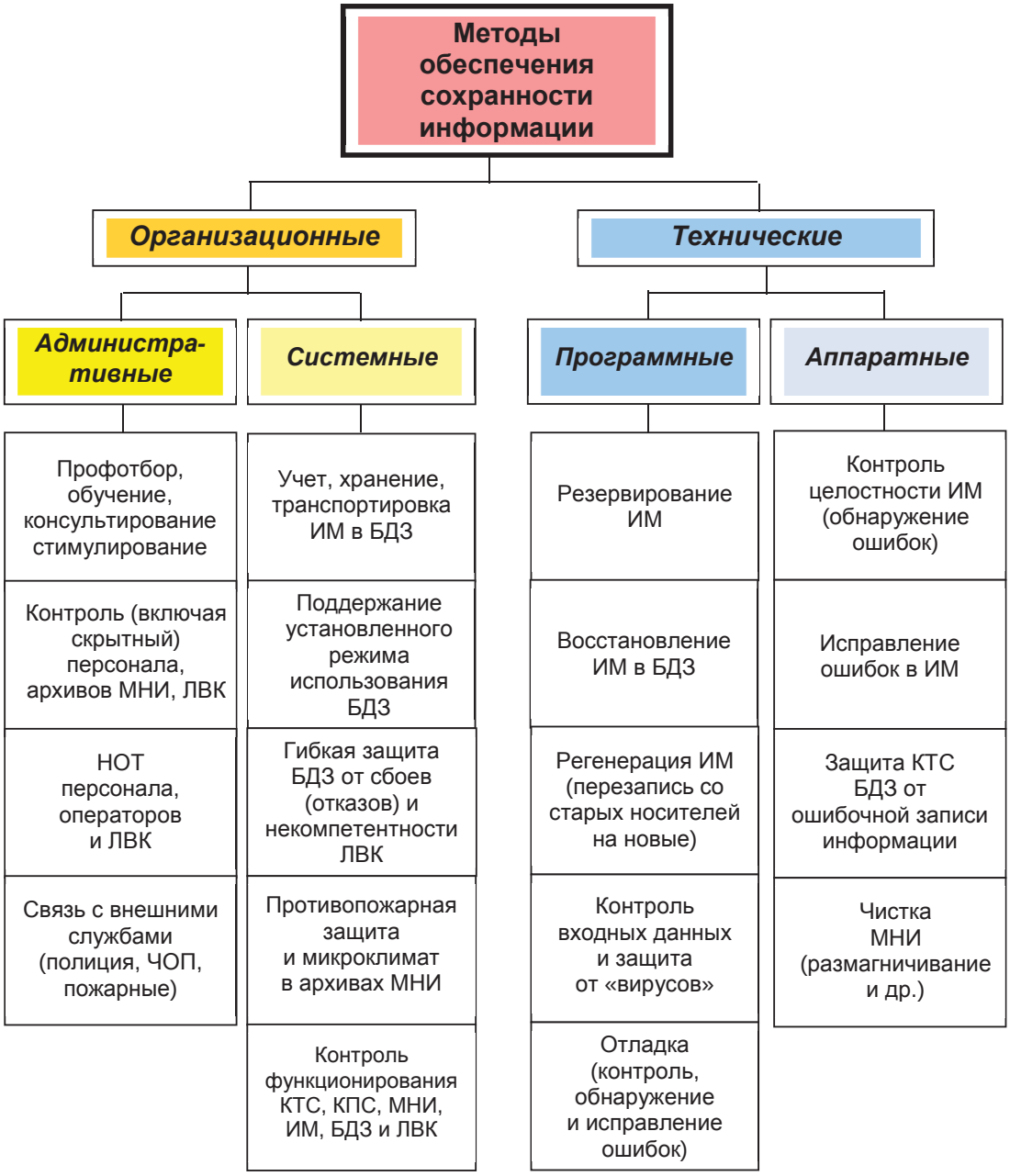

Рис. 5. Общая классификация методов обеспечения (повышения) сохранности информации в эргасистемах

минимизация сведений и данных, доступных персоналу;

минимизация связей (контактов) персонала;

дублирование контроля важных операций (обеспечивает, кроме того, повышение надежности выполнения ответственных операций, и, как следствие, уровня сохранности информации).

Существует также большое количество *аппаратных* (схемных) методов обнаружения ошибок и искажений ИМ (см. *рис.* 5) путем контроля магнитных носителей информации (МНИ), причем при рациональной комбинации подобных методов можно решить задачу защиты ИМ от разрушения при эксплуатации. Данные методы реализуются, как правило, в аппаратном варианте, но часто и в виде программных модулей.

Получение контрольных сумм. В качестве дополнительной избыточной информации для проверки *целостности* ИМ может использоваться сумма всех символов (хранимая в конце ИМ), полученная циклическим сложением после обновления на законном основании. Может также использоваться обратная величина контрольной суммы, при этом сумма всей информации блока ИМ и обратной величины всегда равна нулю.

Для обнаружения искажающих ИМ M_0 простых перестановок (транспозиции) символов (контрольная сумма остается прежней) на практике используются более сложные алгоритмы подсчета контрольной суммы (например, с учетом номера позиции символа). Кроме того, с целью скрытия значения контрольной

суммы она может подвергаться различным защитным преобразованиям.

Использование контрольных чисел. В качестве дополнительной избыточной информации для проверки целостности ИМ может использоваться цифра (хранимая в конце ИМ), связанная с символами ИМ некоторым соотношением. Например, контрольной цифрой может быть остаток от деления контрольного числа на 11, если используется схема сравнения по mod 12.

Использование избыточных кодов — обычно в конце ИМ большого размера вводятся дополнительные контрольные биты (8 или 16), которые позволят выявить, а иногда и автоматически исправить имеющиеся в ИМ ошибки. Схемы, реализующие данный метод, наиболее сложны.

Для магнитных дисков и барабанов *защита записи* обычно проводится на уровне дорожек и на уровне физической записи. Разрешение или запрещение записи на всех дорожках осуществляется *специальными переключателями* на панели управления накопителями. Для частичной защиты жесткого МНИ (диска) обычно его разбивают (с помощью специальных программ) на несколько частей — «самостоятельных» (логических) дисков со своими именами. При этом некоторые из них временно делают доступными только для чтения, чтобы защитить ИМ от изменения, в частности, от «заражения» или порчи «компьютерным вирусом»[15] [17].

Для магнитных флеш-накопителей и карт памяти с этой целью используется переключатель для блокировки устройства от записи, обеспечивающий защиту от несанкционированных корректировок, ошибочных действий, «вирусов» и др. и сохранность программ и данных, которые используются без изменений. Для гибких магнитных дисков — используется специальная *прорезь защиты* (если эту прорезь заклеить, то на дискету нельзя будет произвести запись).

Для магнитных лент используется специальное кольцо защиты от случайной или некомпетентной записи, при отсутствии которого запись на ленту невозможна, поскольку кнопка, отключающая при нажатии схему защиты записи, входит в освободившееся от кольца концентрическое пространство катушки.

Программная проверка по четности, использующая специальную команду «чтение с контролем», реализует контроль только что записанных ИМ без их пересылки в оперативное запоминающее устройство и обеспечивает более качественный контроль по сравнению со *схемной проверкой четности* для каждого бита (слова) при считывании (так как последняя не выявляет ошибок в случае четного количества неверных битов). Частные случаи метода: проверка горизонтальной четности с помощью одного контрольного символа (слова) в конце записи (блока записей); проверка диагональной четности — биты четности соответствуют четности, подсчитываемой по всем диагональным линиям.

Использование счетчиков и порядковых номеров при вводе-выводе и подготовке ИМ. При выполнении операций ввода-вывода обычно подсчитываются ЕМИ (информационные блоки, записываемые на магнитный носитель, считываемые перфокарты и др.). Итоговое значение счетчика документируется и добавляется в ИМ (файл) с целью контроля. При подготовке ИМ на перфокартах с целью контроля полноты файла или выявления нарушений в порядке следования перфокарты нумеруются.

Контроль верности входных ИМ используется в программах ЛВК.

Алгоритмы, реализующие данный метод, достаточно просты. Например, проверку значений цифровых данных осуществляют на основе контроля допустимого диапазона изменения некоторого количественного показателя (например, вероятность не может быть равна 1,5; скорость движения управляемых объектов не может превышать 3×10^6 *м/с* и др.) или показателя логичности (количество решаемых функциональной подсистемой эргасистемы задач не может быть меньше количества ее функций).

Методы восстановления информации в буферном запоминающем устройстве эргасистемы предусматривают использование резервных ИМ, хранящихся на носителях различного типа и вида (магнитных дисках, магнитных барабанах, магнитных лентах, перфокартах и пр.) [3]. Традиционным для МНИ является ***метод восстановления с циклическим оперативным копированием*** ИМ (через определенные промежутки времени) на контрольные носители по схеме «дед — отец — сын». ИМ «сын» (M_0) является последней текущей версией, ИМ «отец» (предыстория Π_{-1} ИМ M_0) отличается от предыдущего на одну выполненную работу с ИМ, а ИМ «дед» (предыстория Π_{-2} ИМ M_0) — на две.

Выбор метода восстановления ИМ определяется структурой эргасистемы, типом контроля, организацией файлов, частотой обновления, соотношением объемов используемых и неиспользуемых данных, ценностью информации, максимально допустимым временем восстановления и др.

При повышенных требованиях к *сохранности* информации может возникнуть необходимость в использовании более одной резервной копии ИМ, которые должны храниться в специальном безопасном месте.

Для повышения уровня *целостности* ИМ в БДЗ используется также большой набор вспомогательных программ обслуживания БДЗ (некоторые из них могут не включаться в СУБД)[16]:

ведения системного журнала КСА (фиксирования сведений об изменениях ИМ для упрощения контроля сохранности БДЗ);

разгрузки (копирования БДЗ для последующего ее восстановления);

восстановления (возврата содержимого БДЗ и системного журнала в начальные до внесения изменений

[15] Ловцов Д. А. Защита информации от компьютерных вирусов // Информатика и образование. 1996. № 4. С. 121—128.

[16] Шураков В. В. Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1985. 224 с.

состояния после сбоев КСА по копиям, полученным в результате работы программы разгрузки);

отката (возврата в исходное положение БДЗ в результате фиксирования незаконных или ошибочных операций над ИМ);

контрольных точек и повторного исполнения (отката только до последней контрольной точки вместо возвращения на общее начало с целью уменьшения непроизводительных затрат времени);

выявления нарушений ограничений *целостности* БДЗ после каждого внесения изменений в ИМ с вызовом программ отката для выхода на исходный рубеж и печатью сообщения об ошибке.

Распределение методов и процедур обеспечения защищенности информации в сети эргасистемы

К штатным аппаратно-программным процедурам (номера приведены в *таблице*) ОЗИ информационно-распределительной сети эргасистемы относятся следующие[17] [2].

1. Криптографическое преобразование (для обеспечения скрытности информационного массива-сообщения (ИМ) или информации о трафике, а также для дополнения ряда других процедур защиты). Возможны симметричное (с использованием тайных ключей) и асимметричное (с использованием известного и индивидуального ключей) преобразования ИМ. При этом степень защиты при помощи криптографического преобразования в значительной мере определяется способом распределения ключей.

2. Управление доступом (для предотвращения несанкционированных попыток доступа к ресурсам подсети, выдачи предупреждения ЛВК (субъекту доступа), и регистрации события в системном журнале для последующего анализа). Используется идентификация логического объекта или информация о нем (пароль и др.) для проверки его полномочий.

3. Обеспечение целостности информационных массивов (массивов данных и программных массивов). Целостность ИМ обеспечивается добавлением к нему при передаче величины, которая является функцией самих данных. На принимающей стороне генерируется такая же величина и сравнивается с принятой. Обнаружение на соответствующем уровне архитектуры взаимодействия абонентов сети несовпадения двух величин может вызвать выполнение процедуры восстановления на этом же или более высоком уровне.

4. Обмен «идентификацией» (для установления или отклонения (завершения) соединения пары информационных узлов (эргасистем) с выдачей сообщения о соответствующем событии). Используются пароли, криптоалгоритмы в сочетании с протоколами «рукопожатия» или взаимной идентификации и аутентификации (для защиты от переадресации), а также характеристики и взаимоотношения подчиненности логических объектов.

5. Заполнение трафика или маскирующий обмен (для защиты от попыток анализа трафика). Процедура эффективна только в случае преобразования всего трафика, когда нельзя отличить информацию от заполнения.

6. Управление маршрутизацией (для использования только безопасных с точки зрения защиты информации подсетей, участков приема, звеньев). Возможно запрещение передачи некоторых ИМ по определенным маршрутам. Оконечный абонент, обнаружив манипуляцию с его ИМ, может потребовать изменить маршрут доставки данных.

7. Цифровая сигнатура. Процесс формирования сигнатуры ИМ при передаче основан на вычислении его криптографической контрольной суммы с использованием индивидуального ключа субъекта (или на преобразовании ИМ). При проверке сигнатуры в принятом ИМ используются типовые (общепринятые) процедуры и информация, из которых нельзя получить привилегированную информацию первого процесса. Существенной характеристикой этого процесса является то, что сигнатура может быть проверена впоследствии третьей стороной.

8. «Нотариальное» заверение (для подтверждения целостности ИМ, удостоверения абонента-источника и абонента-получателя ИМ, регистрации времени сеанса связи и др.), обеспечивается третьей стороной — «нотариусом».

9. Фильтрация информации по принятым в эргасистеме правилам. Основными средствами являются сетевые защищенные экраны (брандмауэры), применяемые на канальном (экранирующий *концентратор*), сетевом (экранирующий *маршрутизатор*), транспортном (транспортный экран) и прикладном (прикладной *экран*) уровнях, обеспечивая предотвращение НСД к ресурсам подсети извне.

Как видно из *таблицы*, на двух нижних уровнях применяется только «позвенное» или канальное (*link-by-link*) преобразование потока данных (т. е. проходящих через звено — *data link*), реализуемое с помощью протокола канального уровня. Способ «позвенного» преобразования имеет следующие особенности:

защищается вся передаваемая по каналу связи информация, включая служебную;

вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;

все передаваемые ИМ оказываются открытыми на промежуточных узлах — ретрансляторах, шлюзах и др.;

субъект не принимает участия в выполняемых операциях;

для каждой пары узлов требуется свой ключ;

алгоритм шифрования должен обладать достаточно высокой стойкостью и обеспечивать скорость шифрования на уровне пропускной способности канала,

[17] Методические материалы и документация по пакетам прикладных программ. Вып. 57. Телеобработка данных и вычислительные сети / Под ред. В. П. Данилочкина, В. К. Щербо. М. : МЦНТИ, 1988. 342 с.; Ловцов Д. А. Распределение методов и процедур обеспечения за¬щищённости информации в АСУ // Вопросы защиты информации. 1996. № 4. С. 20—24.

Таблица

Распределение методов и процедур КЗИ по стандартизованным уровням *ISO/OSI* архитектуры сети эргасистемы

Уровень	Основные функции	Штатные процедуры	Целесообразные методы
7	Информационно-логическая обработка ИМ для решения практических задач Хранение ИМ в архивах и в базе данных и знаний (БДЗ) Выбор средств и передача ИМ. Доступ к БДЗ	— — **1—5, 7, 8, 9**	Оптимизация структур переработки информации. Контроль преобразований. Резервирование и регенерация ИМ. Восстановление ИМ в БДЗ. Отладка и тестирование комплекса программ. НОТ персонала эргасистемы. Физическая изоляция. Профилактика «компьютерных вирусов». Преобразование файлов.
6	Выбор формы представления (*ASCII, EBCDIC* и др.) Сжатие данных (наборов одинаковых кодов) Защитное преобразование	**1**	Защитные преобразования ИМ субъектов
5	Соединение с программой субъекта. Синхронизация служебных ИМ. Обработка приоритетов и прерываний.	—	Идентификация программных компонентов. Автоматическая регистрация прерываний
4	Установление связи по каналу. Установление соответствия между адресами и сетевыми именами абонентов.	**1—4, 7, 9**	
3	Маршрутизация (по адресу) в сети (подсети) эргасистемы.	**1—7, 9**	Реконфигурация подсетей ИРС, адаптивная к отказам и сбоям.
2	Установление связи между соседними информационными узлами. Обнаружение ошибок при передаче данных между соседними узлами.	**1, 9**	
1	Выбор формы сигнала — переносчика ИМ.	**1**	Экранирование кабеля.

иначе возникнет задержка сообщений, которая может привести к блокировке информационного узла (эргасистемы) или существенному снижению его производительности. Это можно обеспечить путем аппаратной реализации алгоритма, что, однако, увеличивает расходы на создание и обслуживание узла.

Сетевой уровень обеспечивает больше услуг по КЗИ, поскольку на нем сосредоточено управление маршрутизацией. Эти услуги обеспечиваются протоколами доступа к подсети, маршрутизации и трансляции. Управление доступом на сетевом уровне позволяет отклонять несанкционированные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня.

На *транспортном* уровне осуществляется защита индивидуальных транспортных соединений. На *сеансовом* уровне КЗИ не предусмотрены. На уровне *представления* осуществляется защитное преобразование ИМ ЛВК. *Прикладной* уровень может обеспечить любую услугу по защите информации, хотя некоторые из них обеспечиваются на основе методов, реализуемых на более нижних уровнях. ЛВК сами могут предпринять дополнительные меры по защите своей информации, например, использовать «межоконечное» (*end-to-end)* преобразование на более высоких уровнях.

Выбор и применение других методов и средств КЗИ (см. *табл.*) в сети эргасистемы (на уровне прикладных процессов, на уровнях взаимодействия информационных узлов) должны осуществляться с учетом требований к степени безопасности информации в конкретной сети, структур и принципов оптимизации переработки информации в ИРС эргасистемы[18] [6, 8].

Таким образом, рассмотрена непротиворечивая совокупность и рациональное распределение прагматических методов и целесообразных сетевых аппаратно-программных процедур обеспечения защищенности информации в эргасистемах на основе применения соответствующих принципов контроля и защиты информации от ошибок переработки, разрушающих факторов, несанкционированного доступа и использования.

[18] Ловцов Д. А. Методы защиты информации в АСУ сложными динамическими объектами // НТИ. Сер. 3. Информ. процессы и системы. 2000. № 5. С. 29—45; Защита информации в глобальной сети Интернет // Информатика и образование. 1998. № 5. С. 101—108; Защита информации в информационно-вычислительной сети // НТИ. Сер. 3. Информ. процессы и системы. 1997. № 2. С. 7—13.

Литература

1. Зубов А.Ю. Криптографические методы защиты информации. М. : Гелиос АРВ, 2005. 192 с.
2. Конахович Г.С. Защита информации в телекоммуникационных системах. М. : МК Пресс, 2005. 288 с.
3. Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. М. : Синтег, 2004. 496 с.
4. Ловцов Д.А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере. II. Качество информации // Правовая информатика. 2015. № 2. С. 53—61.
5. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
6. Ловцов Д.А. Информационная теория эргасистем : монография. М. : Росс. гос. ун-т правосудия, 2021. 250 с.
7. Ловцов Д.А. Принципы обеспечения защищенности информации в эргасистемах // Правовая информатика. 2021. № 1. С. 36—50.
8. Ловцов Д.А., Галахова А.Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2012. № 4. С. 13—20.
9. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 3. Информ. процессы и системы. 2006. № 9. С. 1—9; Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ. Сер. 3. Информ. процессы и системы. 2005. № 3. С. 1—7.
10. Ловцов Д.А., Князев К.В. Защищенная биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2014. № 2. С. 100—103; II. Качество информационно-математического обеспечения // Информация и космос. 2014. № 3. С. 95—100.
11. Ловцов Д.А., Сухов А.В., Зайцев М.А., Глинский И.В. Информационно-математический подход к киберзащите информационных систем с использованием энтропии покрытия // Вестник Росс. нового ун-та. Сер. «Сложные системы: модели, анализ и управление». 2016. № 1-3. С. 150—157.
12. 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.
13. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М. : Академия, 2009. 336 с.
14. Основы технической эксплуатация радиотехнических систем специального назначения / Ратушняк В.Н., Хоменко И.В., Малыков К.А. и др. Под ред. К.А. Малыкова. Красноярск : Сиб. фед. ун-т, 2015. 335 с.
15. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. СПб. : Питер, 2008. 272 с.
16. Солодовников В.И. Регистры сдвига и криптоалгоритмы на их основе. Берлин : LAP LAMBERT Academic Publishing, 2017. 112 с.
17. Файтс Ф., Джонстон П., Кратц М. Компьютерный вирус: проблемы и прогноз. М. : Мир, 2013. 176 с.
18. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М. : ДМК Пресс, 2008. 544 с.
19. Шнайер Б. Прикладная криптография. М. : Триумф, 2013. 518 с.

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

METHODS AND PROCEDURES FOR 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, Moscow, Russian Federation.*
E-mail: dal-1206@mail.ru

Keywords: *ergasystem, information security, reliability, confidentiality, integrity, methods of ensuring, hardware and software procedures, information distribution network, pragmatic classification, indicators, criteria, information control and protection subsystem, organisational and functional principles.*

Abstract.

Purpose of the paper: improving the scientific and methodological basis of the theory of information security in ergasystems.

Methods used: system analysis, complex task formalisation, pragmatic classification and distribution of the basic methods and hardware and software procedures for ensuring information security in ergasystems.

Results obtained: the mathematical structure of the multi-faceted task of ensuring information security in ergasystems was determined. The logical sequence of methodological stages of development of the information control and protection subsystem based on pragmatic organisational and functional principles was determined. A justification was given for a noncontradictory corpus of methods of information control and protection against processing errors, destructive factors, and unauthorised access and use. A justification was given for a pragmatic classification of the basic methods and a distribution of appropriate hardware and software procedures for ensuring information security in ergasystems.

The obtained results are a conceptual and theoretical foundation for setting up efficient information and mathematical support for information control and protection in ergasystems.

References

1. Zubov A.Iu. Kriptograficheskie metody zashchity informatsii. M. : Gelios ARV, 2005. 192 pp.
2. Konakhovich G.S. Zashchita informatsii v telekommunikatsionnykh sistemakh. M. : MK Press, 2005. 288 pp.
3. Kul'ba V.V., Kovalevskii S.S., Shelkov A.B. Dostovernost' i sokhrannost' informatsii v ASU. M. : Sinteg, 2004. 496 pp.
4. Lovtsov D.A. Lingvisticheskoe obespechenie pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. II. Kachestvo informatsii. Pravovaia informatika, 2015, No. 2, pp. 53-61.
5. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74.
6. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : Ross. gos. un-t pravosudiia, 2021. 250 pp.
7. Lovtsov D.A. Printsipy obespecheniia zashchishchennosti informatsii v ergasistemakh. Pravovaia informatika, 2021, No. 1, pp. 36-50.
8. Lovtsov D.A., Galakhova A.E. Zashchita intellektual'noi sobstvennosti v seti Internet. Informatsionnoe pravo, 2012, No. 4, pp. 13-20.
9. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. NTI, ser. 3, Inform. protsessy i sistemy, 2006, No. 9, pp. 1-9; Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. NTI, ser. 3, Inform. protsessy i sistemy, 2005, No. 3, pp. 1-7.
10. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2014, No. 2, pp. 100-103; II. Kachestvo informatsionno-matematicheskogo obespecheniia. Informatsiia i kosmos, 2014, No. 3, pp. 95-100.
11. Lovtsov D.A., Sukhov A.V., Zaitsev M.A., Glinskii I.V. Informatsionno-matematicheskii podkhod k kiberzashchite informatsionnykh sistem s ispol'zovaniem entropii pokrytiia. Vestnik Ross. novogo un-ta. Ser. "Slozhnye sistemy: modeli, analiz i upravlenie", 2016, No. 1-3, pp. 150-157.
12. 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.
13. Mel'nikov V.P., Kleimenov S.A., Petrakov A.M. Informatsionnaia bezopasnost' i zashchita informatsii. M. : Akademiia, 2009. 336 pp.
14. Osnovy tekhnicheskoi ekspluatatsiia radiotekhnicheskikh sistem spetsial'nogo naznacheniia. Ratushniak V.N., Khomenko I.V., Malykov K.A. i dr. Pod red. K.A. Malykova. Krasnoiarsk : Sib. fed. un-t, 2015. 335 pp.
15. Rodichev Iu.A. Informatsionnaia bezopasnost': normativno-pravovye aspekty. SPb. : Piter, 2008. 272 pp.
16. Solodovnikov V.I. Registry sdviga i kriptoalgoritmy na ikh osnove. Berlin : LAP LAMBERT Academic Publishing, 2017. 112 pp.
17. Faits F., Dzhonston P., Kratts M. Komp'iuternyi virus: problemy i prognoz. M. : Mir, 2013. 176 pp.
18. Shan'gin V. F. Zashchita komp'iuternoi informatsii. Effektivnye metody i sredstva. M. : DMK Press, 2008. 544 pp.
19. Shnaier B. Prikladnaia kriptografiia. M. : Triumf, 2013. 518 pp.