ВЕСТНИК
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
МОРСКОГО И РЕЧНОГО ФЛОТА ИМЕНИ АДМИРАЛА С. О. МАКАРОВА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И АВТОМАТИЗАЦИЯ НА ТРАНСПОРТЕ

УДК 004.056.53 : 004.4

А. Н. Люльченко,
А. П. Ныpков,
В. Г. Швед

МОДЕЛЬ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ТРАНСПОРТЕ

В статье рассматриваются особенности моделирования системы обеспечения информационной безопасности (СОИБ) на объектах защиты органов управления транспортом. В качестве основных отличительных факторов выделены достаточно большое многообразие и разнородность СОИБ и обрабатываемой информации в них. Исследование СОИБ возможно с использованием методов моделирования процессов их функционирования. В качестве математической схемы для описания динамики системы обеспечения информационной безопасности предлагается дискретный метод представления процессов обеспечения информационной безопасности, который соответствует их содержанию и значительно облегчает их математическое описание. Показано, что важнейшим этапом, оказывающим влияние на качество принимаемого решения при управлении информационной безопасностью организации, является оценка фактического состояния системы обеспечения информационной безопасности. Представленная система отображений позволяет выявить взаимозависимость и взаимовлияние различных факторов, оказывающих воздействие на систему обеспечения информационной безопасности организации, и служит методологической базой для разработки конкретных методик. Процесс разработки формальной схемы позволяет структурировать и четко сформулировать суть задачи оценки состояния системы обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, модель, формализация, управление, информационная система, оценка состояния.

В НАСТОЯЩЕЕ время Министерством транспорта Российской Федерации и подведомственными ему федеральными агентствами и службой создается система информационного обеспечения безопасности населения на транспорте. Эта система осуществляет интеграцию информационных ресурсов органов исполнительной власти всех уровней в области обеспечения транспортной безопасности в единое защищенное закрытое информационное пространство [1]. В рамках системы информационного обеспечения безопасности населения на транспорте создается Единая государственная информационная система обеспечения транспортной безопасности (ЕГИС ОТБ). Укрупненная структура ЕГИС ОТБ представлена на рис. 1. Как видно, она представляет собой трехуровневую систему: на первом уровне находятся объекты информатизации (ОИ) Минтранса России; на втором уровне — ОИ подведомственных агентств и службы (шесть объектов); на нижнем уровне — ОИ территориальных органов федеральных агентств и службы (31 объект) [1]. В структурных подразделениях Минтранса России, подведомственных агентствах и службе, территориальных органах федеральных агентств и службы (далее — организации) осуществляется обработка персональных данных как своих сотрудников (в кадровых подразделениях и бухгалтериях), так и пассажиров, а также возможна обработка служебной и другой информации ограниченного доступа [2], [3].

Скопление больших объемов информации приводит к увеличению вероятности утечки информации ограниченного доступа, а значит, и к необходимости принятия мер по обеспечению безопасности информации. Совершенствуются средства и способы несанкционированного доступа к информации, ее искажения, уничтожения или подмены. К этим проблемам обеспечения безопасности обрабатываемой информации добавляются вопросы защиты в каналах передачи данных и в мультисервисных сетях транспортной отрасли [4] — [7]. В связи с этим появляется необходимость в постоянном совершенствовании способов и средств обеспечения информационной безопасности [8] — [13]. В указанных организациях объектами защиты являются [11]:

– информация, обрабатываемая и содержащаяся в информационных системах;

– технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации);

– общесистемное, прикладное, специальное программное обеспечение;

– информационные технологии, а также средства защиты информации.

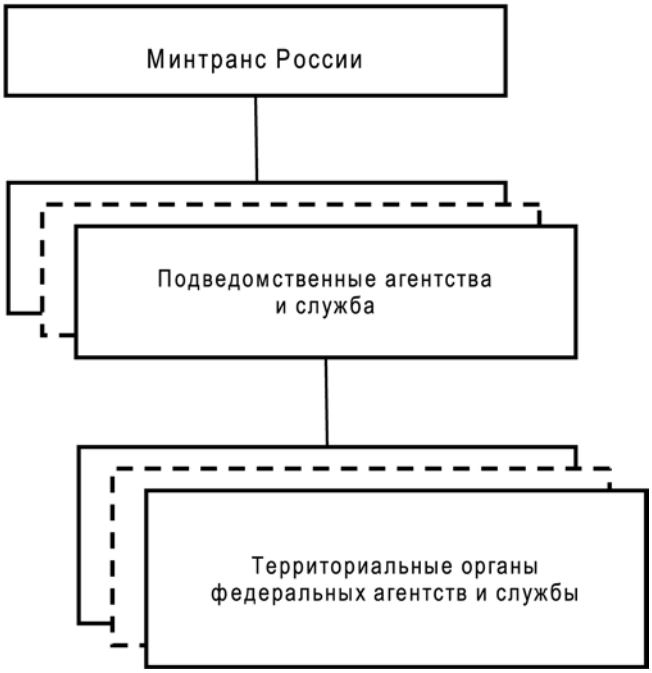

Рис. 1. Структура единой государственной информационной системы обеспечения транспортной безопасности

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью с целью защиты информации от широкого диапазона угроз для обеспечения конфиденциальности, целостности и доступности информации в организациях [14], [15]. Для обеспечения выполнения требований по конфиденциальности, целостности и доступности информации в рамках ЕГИС ОТБ должна создаваться система обеспечения информационной безопасности и соответствующая ей система управления информационной безопасностью (СУИБ).

Специфическими особенностями при решении задач создания системы обеспечения информационной безопасности (СОИБ) являются:

– неполнота и неопределенность исходной информации о характерных угрозах информационной безопасности;

– многокритериальность задачи создания и оценки состояния СОИБ, связанная с необходимостью учета большого числа частных показателей (требований) системы обеспечения информационной безопасности;

– наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СОИБ;

– невозможность применения классических методов оптимизации.

Следовательно, система обеспечения информационной безопасности является носителем свойств сложной системы. Определение оптимальных (рациональных) вариантов ее построения и обеспечения результативности мероприятий по нейтрализации угроз информационной безопасности может быть выполнено при тщательном и глубоком знании ее функционирования, что обуславливает необходимость использования методов математического моделирования. Практическая

задача обеспечения информационной безопасности состоит в разработке модели представления системы информационной безопасности, которая позволяла бы решать задачи создания, использования и оценки эффективности СОИБ как для проектируемых, так и существующих систем.

В качестве математической схемы для описания динамики системы обеспечения информационной безопасности примем дискретный метод представления процессов обеспечения информационной безопасности. Под процессом обеспечения информационной безопасности будем понимать совокупность последовательных действий, направленную на достижение требуемой защищенности информации и информационной структуры организации от актуальных угроз безопасности информации. Представление функционирования СОИБ как конечного дискретного процесса соответствует его содержанию и значительно облегчает его математическое описание.

В общем случае элементами внутреннего состояния системы обеспечения информационной безопасности являются органы управления R, организационно-распорядительные документы D, а также средства обеспечения информационной безопасности Z. Средства обеспечения информационной безопасности включают технологии, физические, технические, программные, криптографические, правовые, организационные средства, а также средства сбора, формирования, обработки, передачи или приёма информации о состоянии информационной безопасности организации и мерах по её совершенствованию.

Под внутренним состоянием элементов системы обеспечения информационной безопасности будем понимать векторы S^R, S^D, S^Z, определенные на области возможных значений параметров описания элементов R, D и Z соответственно. Тогда матрица внутреннего состояния элементов СОИБ будет определяться вектором $S = (S^R, S^D, S^Z)$.

В свою очередь, состояние системы обеспечения информационной безопасности зависит от [16]:

– множества угроз информационной безопасности актуальных для данной организации $W = \{W^A, W^T\}$, где W^A, W^T — множества антропогенных и техногенных угроз информационной безопасности;

– множества требований, предъявляемых к системе обеспечения информационной безопасности $P = \{P^R, P^D, P^Z\}$, где P^R, P^D, P^Z — множества требований, предъявляемых к состоянию элементов R, D и Z системы S соответственно;

– множества управляющих воздействий на элементы системы обеспечения информационной безопасности $U = \{U_l\}$, где U_l — значение управляющего параметра, определяющего характер функционирования l-го элемента СОИБ.

Переменные S, W, P образуют многомерное пространство состояния системы обеспечения информационной безопасности. Точку $G = (S, W, P)$ в этом пространстве назовем состоянием системы обеспечения информационной безопасности. Тогда процесс функционирования СОИБ можно представить через изменение во времени ее состояния: $G = (S, W, P)$.

Для описания динамики состояния системы обеспечения информационной безопасности примем дискретный метод представления процессов обеспечения информационной безопасности. Такое представление функционирования СОИБ, как правило, соответствует его содержанию и особенно периодичности контроля (аудита), а также позволяет упростить его математическое описание. Описание процессов функционирования СОИБ дискретной математической схемой представляет собой временную последовательность состояний системы, определяемую положением точки G в многомерном пространстве параметров ее состояния.

С учетом ранее изложенного, выражение, описывающее движение точки G во времени, имеет следующий вид:

$$G(0), F_1 : \{G(0)\} \to G(1), F_2 : \{G(1)\} \to G(2), .., F_n : \{G(n-1)\} \to G(n), .., F_N : \{G(N-1)\} \to G(N).$$

Для упрощения дальнейшего анализа будем полагать, что операторы преобразования F_n не зависят от времени, а зависят от n-го номера шага процесса функционирования системы обеспечения информационной безопасности. Примем, что $F : \{G(n)\}, \forall n \in 1..N$ есть процесс функци-

онирования СОИБ, где n — номер шага процесса, а N — число шагов, определяющих рассматриваемую продолжительность функционирования системы. Изменение состояния СОИБ представляет собой функцию управления $G(n) = G_U(U(n))$. На любом n-м шаге процесса поведение системы обеспечения информационной безопасности определяется вектором управления $U = (U_l)$.

Изменение состояния СОИБ определяется изменением модели угроз информационной безопасности, функционированием ее элементов и их взаимодействием в процессе этого функционирования в соответствии с управляющими воздействиями, которые формируются СУИБ. В ходе функционирования элементы системы обеспечения информационной безопасности меняют свое внутреннее состояние, следовательно, для дискретного описания процесса изменения состояния СОИБ $G(n)$ необходимо определить последовательность изменения составляющих состояния на каждом n-м шаге процесса ее функционирования.

С учетом содержания процессов функционирования СОИБ последовательность изменения состояния $G(n)$ может быть представлена следующим образом. На $(n + 1)$ шаге изменяются угрозы информационной безопасности $W(n + 1)$, что обуславливает изменение требований к системе обеспечения информационной безопасности $P(n + 1)$. С появлением новых требований осуществляется оценка соответствия состояния СОИБ предъявляемым требованиям и вырабатываются управляющие воздействия $U(n + 1)$ на изменение внутреннего состояния элементов $S = \{S^R, S^D, S^Z\}$ системы обеспечения информационной безопасности с целью нейтрализации новых угроз информационной безопасности. Тем самым формируется вектор внутреннего состояния $S(n + 1)$ на $(n + 1)$-м шаге процесса ее функционирования.

Представим процесс $F : \{G(n)\} \to G(n+1)$ изменения состояния и управления системы на $(n + 1)$-м шаге следующей системой операторов:

$$M_1 : \{W(n), P(n), U(n), S(n)\} \to W(n+1);$$

$$M_2 : \{W(n+1), P(n), U(n), S(n)\} \to P(n+1);$$

$$M_3 : \{W(n+1), P(n+1), U(n), S(n)\} \to U(n+1);$$

$$M_4 : \{W(n+1), P(n+1), U(n+1), S(n)\} \to S(n+1).$$

Оператор преобразования F представляет собой последовательность операторов M_1, M_2, M_3, M_4.

Следующим шагом формализации процессов обеспечения информационной безопасности является описание управляющих воздействий $U = (U_l)$, вырабатываемых системой управления информационной безопасностью.

Деятельность службы обеспечения информационной безопасности в общем случае представляет собой приведенную последовательность действий:

– сбор информации о состоянии системы обеспечения информационной безопасности;

– оценка состояния системы обеспечения информационной безопасности;

– разработка плана деятельности организации по совершенствованию СОИБ;

– выработка управляющих воздействий.

Для осуществления деятельности службы обеспечения информационной безопасности необходимо фактическое состояние системы G перевести в его информационный образ G^{Φ}:

$$M_5 : \{G\} \to G^{\Phi},$$

где $G^{\Phi} = \{W^{\Phi}, P^{\Phi}, S^{\Phi}\}$.

Следовательно, должен существовать некоторый оператор отображения M_6, предназначенный для формирования информационного образа о фактическом состоянии системы обеспечения информационной безопасности G^I на момент $n = 0$:

$$M_6 : \{G^{\Phi}, Q\} \to G^I,$$

где Q — множество показателей качества системы, $Q = \{Q^R, Q^D, Q^Z\}$, Q^R, Q^D, Q^Z — множества показателей качества элементов R, D и Z системы S соответственно.

Множество G^I представляет собой состояние системы обеспечения информационной безопасности, исходя из которого принимается решение для изменения системы $S = \{S^R, S^D, S^Z\}$. Оператор M_6 имеет важное значение в деятельности службы обеспечения информационной безопасности, так как от качества его реализации зависит полнота отображения состояния СОИБ $G_{\text{п}}^{\text{ф}}$:

$$M_6 : \{G_{\text{п}}^{\text{ф}}, Q\} \to G^I \equiv G.$$

Важнейшим этапом, оказывающим влияние на качество принимаемого решения, является оценка фактического состояния СОИБ [17], [18]. В оценку состояния системы O^S входят: параметры элементов системы обеспечения информационной безопасности S; перечень актуальных угроз информационной безопасности W и возможный ущерб $Y = \{Y_i\}$ от их реализации; состояние информационной инфраструктуры организации S^I, $S^I = \{S^I_i\}$, где S^I_i — параметры информационных систем, осуществляющих обработку информации в организации; требования, предъявляемые к СОИБ, $P = \{P^R, P^D, P^Z\}$. Оценку состояния системы обеспечения информационной безопасности можно представить оператором вида

$$M_7 : \{W, Y, S^I, P, Q, S\} \to O^S.$$

Тогда процесс получения информационного образа и оценка состояния системы определяется последовательностью следующих операторов:

$$M_5 : \{G\} \to G^{\Phi};$$

$$M_6 : \{G_{\text{П}}^{\Phi}, Q\} \to G^I;$$

$$M_7 : \{W, Y, S^I, P, Q, S\} \to O^S.$$

Для формирования информационного образа и оценки состояния системы обеспечения информационной безопасности в организациях проводится аудит информационной безопасности, направленный на выявление несоответствия системы предъявляемым требованиям, выработку решений на устранение существующих противоречий, формирование плана реализации решений [19] — [21].

Рассмотренные свойства СУИБ и принятые предположения позволяют перейти к процессу формализации управления в системе обеспечения информационной безопасности. Процесс функционирования системы управления информационной безопасностью на $(n + 1)$-м шаге может быть представлен следующим отображением:

$$F : \{G(n), U(n)\} \to G(n+1),$$

где $G(n) = (W(n), P(n), U(n), S(n))$ — вектор состояния системы обеспечения информационной безопасности на n-м шаге ее функционирования.

Управление СОИБ представляет собой целенаправленную деятельность. Цели C (например, обеспечение целостности, доступности и конфиденциальности информации), которые задаются на определенный период функционирования системы обеспечения информационной безопасности n^*, т. е. $C(n^*)$. Цель считается достигнутой, если $G(n) \subset C(n^*)$. Управляющие воздействия содержат в себе ограничения, которые определяют параметры системы $G^*(n)$ на период выполнения поставленных задач (например, ограничения на выделение материальных и финансовых ресурсов), а также ограничения на управление $U^*(n)$ (например, последовательность решения, поставленных задач, расхода во времени материальных и финансовых ресурсов). С учетом ранее изложенного управляющее воздействие может быть представление отображением вида:

$$U = \{C(n^*), G^*(n), U^*(n)\}.$$

Процесс принятия решения можно представить как формирование общего плана действий M_8, последовательность процедур во времени и пространстве, в результате реализации кото-

рых достигается цель C, поставленная перед системой обеспечения информационной безопасности (нейтрализация угроз информационной безопасности), а состояние элементов СОИБ приводится в соответствие с требованиями в области обеспечения информационной безопасности $S^{\text{В}} = \{S_{\text{В}}^R, S_{\text{В}}^D, S_{\text{В}}^Z\}$:

$$M_1 : \{W(n), P(n), U(n), S(n)\} \to W(n+1);$$

$$M_2 : \{W(n+1), P(n), U(n), S(n)\} \to P(n+1);$$

$$M_3 : \{W(n+1), P(n+1), U(n), S(n)\} \to U(n+1);$$

$$M_4 : \{W(n+1), P(n+1), U(n+1), S(n)\} \to S(n+1);$$

$$G(n+1) = \{W(n+1), P(n+1), S(n+1)\};$$

$$M_5 : \{G(n+1), U(n)\} \to G^{\Phi}(n+1);$$

$$M_6 : \{G^{\Phi}(n+1), U(n)\} \to G^{I}(n+1);$$

$$M_7 : \{W(n+1), Y(n+1), S^{I}(n+1), P(n+1), S(n+1), O^{S}(n)\} \to O^{S}(n+1);$$

$$M_8 : \{G^{I}(n+1), O^{S}(n+1), U(n), C(n), S^{\text{т}}(n)\} \to C(n+1);$$

$$M_9 : \{G^{I}(n+1), O^{S}(n+1), U(n), C(n+1), S^{\text{т}}(n)\} \to U(n+1);$$

$$M_{10} : \{C(n+1), O^{S}(n+1), U(n+1), S^{\text{т}}(n)\} \to S^{\text{т}}(n+1),$$

где M_{10} — оператор приведения элементов СОИБ в соответствии с требованиями нормативных правовых актов и нормативных документов в области обеспечения информационной безопасности.

Как видно из приведенных операторов, управляющие воздействия направлены на приведение СОИБ в соответствие требованиям, предъявляемым к ней $S^{\text{т}}(n + 1)$. Важнейшим этапом, определяющим эффективность решения, является оценка соответствия системы обеспечения информационной безопасности M_7 предъявляемым требованиям.

Сформулируем постановку задачи реализации оператора формирования управляющих воздействий с учётом положений, изложенных в работе [22]. Пусть в процессе управления информационной безопасностью на $(n + 1)$-м шаге функционирования СОИБ изменились угрозы информационной безопасности $W(n + 1)$, что приводит к изменению требований $P = \{P^R, P^D, P^Z\}$. В результате оценки состояния M_7 фиксируются отклонения отдельных показателей состояния элементов СОИБ: $S = \{S^R, S^D, S^Z\}$, от требуемых значений: $\text{P} = \{P^R, P^D, P^Z\}$. Причины отклонения в результате изменения угроз информационной безопасности $W(n + 1)$ известны, а средства достижения требуемых значений заранее не определены. Такое состояние в управлении информационной безопасностью в дальнейшем понимается как стандартная ситуация в обеспечении информационной безопасности. Оценка состояния осуществляется с учетом системы показателей качества СОИБ: $Q = \{Q^R, Q^D, Q^Z\}$, $Q = Q^R \cup Q^D \cup Q^Z$, $Q = \{q_i\}$, где q_i — единичный показатель качества из множества Q, где $i = \overline{1, N}$, N — количество единичных показателей.

По значениям q_i требуется:

– оценить сложившуюся ситуацию $S = \{S^R, S^D, S^Z\}$ (например, $S_{\text{кр}}$ — критическая, $S_{\text{нд}}$ — неудовлетворительная, $S_{\text{н}}$ — нормальная);

– найти первопричины g_x, обусловившие возникновение S;

– предложить альтернативные решения $\{r_i\}$;

– выбрать и обосновать оптимальное (рациональное) решение R_j.

Цель решения задачи — вернуть СОИБ в состояние нормального функционирования, т. е. отвечающую предъявляемым требованиям: $S^{\text{т}} = \{S_{\text{т}}^R, S_{\text{т}}^D, S_{\text{т}}^Z\}$. При этом может возникнуть два случая.

Первый случай, когда в результате изменения угроз информационной безопасности W система оказывается в критической ситуации. В зависимости от существующих ограничений на G^* и U^* она может быть переведена сразу в состояние нормального функционирования $S_н$ либо сначала в состояние неудовлетворительного функционирования $S_{нд}$, а затем в состояние $S_н$:

$$\Psi(Q) : S_{кр} \rightarrow S_н \cup S_{нд} \rightarrow S_н, S_н \equiv S^т.$$

Второй случай, когда в результате изменения угроз информационной безопасности W система оказывается в состоянии неудовлетворительного функционирования $S_{нд}$. Тогда независимо от существующих ограничений система должна быть переведена в состояние $S_н$:

$$\Psi(Q) : S_{нд} \rightarrow S_н, S_н \equiv S^т.$$

Формула управления упрощенно может быть представлена следующим выражением:

$$\Psi(Q) \subset I(Q), O^S(S), L(g_x), M(R_j),$$

где $I(Q)$ — измерение вектора Q; $O^S(S)$ — оценка ситуации; $L(g_x)$ — поиск показателей первопричин, давших отклонение от требуемых значений; $M(R_j)$ — поиск класса решений R_j. Эта операция последовательно повторяется для уточнения класса R_j и выхода на операцию $R_{опт}$.

Результаты решения задачи могут быть представлены в виде диаграммы, изображенной на рис. 2, где приведен пример оценки состояния защиты ПДн — персональных данных, КТ — коммерческой тайны, СлИ — служебной информации и интегральной оценки состояния информационной безопасности организации [22].

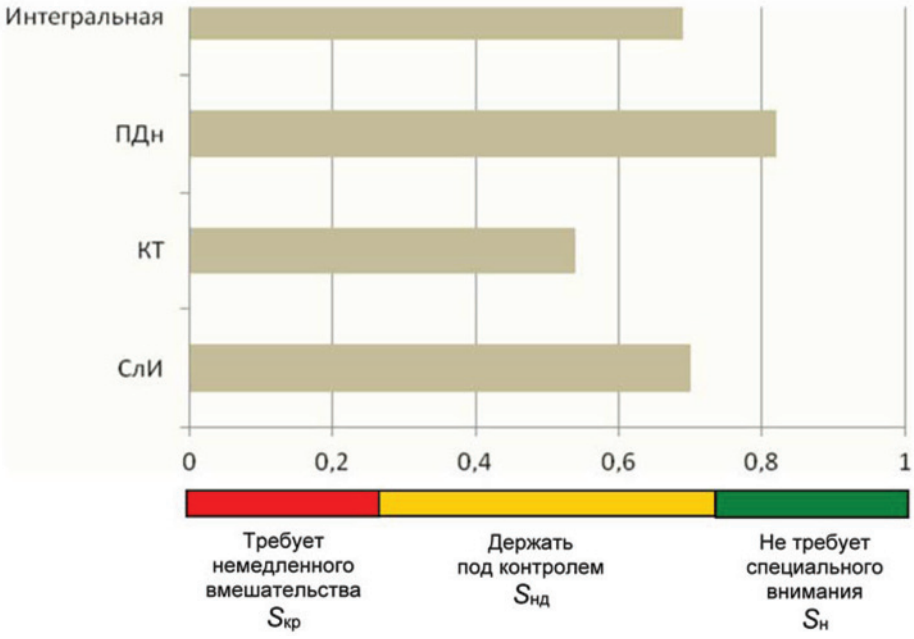

Рис. 2. Диаграмма оценки состояния защиты персональных данных, коммерческой тайны и служебной информации

Таким образом, предлагаемый метод формализованного описания систем обеспечения информационной безопасности способствует созданию четких организационных механизмов управления информационной безопасностью организации. Рассмотренные формальные модели позволяют выявить взаимозависимость и взаимовлияние различных факторов, оказывающих воздействие на систему обеспечения информационной безопасности организации, и служат методологической базой для разработки конкретных методик. Процесс разработки формальной схемы позволяет структурировать и четко сформулировать суть задачи оценки состояния системы обеспечения информационной безопасности. Практическая реализация предложенной модели позволит повы-

сить эффективность системы обеспечения информационной безопасности на этапах ее создания, функционирования и дальнейшего развития.

СПИСОК ЛИТЕРАТУРЫ

1. *Смирнов В. В.* Системы информационного обеспечения безопасности на транспорте / В. В. Смирнов, Е. П. Шабуров [Электронный ресурс]. — Режим доступа: http://federalbook.ru/ files/BEZOPASNOST/soderghanie/NB%20I/VIII/Smirnov.pdf (дата обращения: 29.07.2015).

2. Указ Президента РФ от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/10200083/ (дата обращения: 29.07.2015).

3. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — Режим доступа: http://ivo.garant.ru/#/document/12148555/paragraph/3471:2 (дата обращения: 29.07.2015).

4. *Нырков А. П.* Мультисервисная сеть транспортной отрасли / А. П. Нырков, С. С. Соколов, А. С. Белоусов // Вестник компьютерных и информационных технологий. — 2014. — № 4. — С. 33–38. — DOI: 10.14489/vkit.2014.04. — P. 033–038.

5. *Нырков А. П.* Обеспечение необходимого режима информационной защищенности активов мультисервисной сети транспортной отрасли / А. П. Нырков, С. С. Соколов, Е. А. Мустакаева [и др.] // Проблемы информационной безопасности. Компьютерные системы. — 2014. — № 1. — С. 47–51.

6. *Nyrkov A. P.* Algorithmic support of optimization of multicast data transmission in networks with dynamic routing / A. P. Nyrkov, S. S. Sokolov, A. S. Belousov // Modern Applied Science. — 2015. — Vol. 9. — No. 5. — С. 162–176. — DOI: 10.5539/mas.v9n5p162.

7. *Нырков А. П.* Обеспечение безопасного функционирования мультисервисной сети транспортной отрасли / А. П. Нырков, С. С. Соколов, А. С. Белоусов [и др.] // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2014. — № 2 (32). — С. 143–149.

8. *Запечников С. В.* Информационная безопасность открытых систем: в 2 т. — Т. 1. Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой [и др.] — М.: Горячая Линия – Телеком, 2006. — 536 с.

9. *Соколов С. С.* Модель угроз информационной безопасности организации / С. С. Соколов // Журнал университета водных коммуникаций. — 2009. — № 2. — С. 176–180.

10. *Вихров Н. М.* О безопасности инфраструктуры водного транспорта / Н. М. Вихров, Ю. Ф. Каторин, А. П. Нырков [и др.] // Морской вестник. — 2014. — № 4 (52). — С. 99–102.

11. *Нырков А. П.* Обеспечение безопасности объектов информатизации транспортной отрасли / А. П. Нырков, А. А. Нырков, С. С. Соколов [и др.] — СПб.: Изд-во Политехн. ун-та, 2015. — 544 с.

12. *Мищенко В. И.* Защита информации в государственных информационных системах / В. И. Мищенко, А. К. Шилов // Вестник компьютерных и информационных технологий. — 2015. — №3. — С. 45–47. — DOI: 10.14489/vkit.2015.03. — PP.045–047.

13. *Нырков А. П.* Основные принципы построения защищенных информационных систем автоматизированного управления транспортно–логистическим комплексом / А. П. Нырков, Ю. Ф. Каторин, С. С. Соколов [и др.] // Проблемы информационной безопасности. Компьютерные системы. — 2013. — № 2. — С. 54–58.

14. *Нырков А. П.* Контроль целостности данных при мониторинге транспортных средств / А. П. Нырков, Н. Ю. Вайгандт // Журнал университета водных коммуникаций. — 2013. — № 1. — С. 54–61.

15. *Нырков А. П.* Методика проектирования безопасных информационных систем на транспорте / А. П. Нырков, А. В. Башмаков, С. С. Соколов // Проблемы информационной безопасности. Компьютерные системы. — 2010. — № 3. — С. 58–61.

16. *Язов Ю. К.* Основы методологии количественной оценки эффективности защиты информации в компьютерных системах / Ю. К. Язов. – Ростов н/Д: Изд-во СКНЦ ВШ, 2006. – 274 с.

17. *Хорев А. А.* Оценка эффективности защиты вспомогательных технических средств / А. А. Хорев // Специальная техника. — 2007. — № 2. — С. 48–60; — № 3. — С. 50–63.

18. *Шивдяков Л. А.* Система показателей оценки состояния обеспечения безопасности информации в автоматизированной системе по результатам контроля / Л. А. Шивдяков, И. Н. Бозарный, Ю. К. Язов // Информация и безопасность. — Воронеж: Воронежский гос. техн. ун-т, 2009. — Вып. 2. — С. 251–257.

19. *Ныркov А. П.* Методика аудита объектов информатизации по требованиям информационной безопасности / А. П. Ныркov, С. А. Рудакова // Журнал университета водных коммуникаций. — 2012. — № 3. — С. 146–149.

20. *Жигулин Г. П.* Понятие, основные этапы и виды аудита информационной безопасности на предприятии / Г. П. Жигулин, А. С. Згурский, А. Н. Люльченко // Актуальные проблемы гуманитарных и естественных наук. — 2012. — № 10. — С. 57–60.

21. *Сердюк В. А.* Аудит информационной безопасности – основа эффективной защиты предприятия / В. А. Сердюк // BYTE/Россия. — 2006. — № 4 (92). — С. 32–35.

22. *Макаров А. Д.* Инновационный подход в российской экономике – формальная модель управления информационной безопасностью / А. Д. Макаров, Д. В. Швед, В. Г. Швед // Актуальные направления научных исследований: от теории к практике: материалы V Междунар. науч.-практ. конф. — Чебоксары: ЦНС «Интерактив плюс», 2015. — С. 37–42.

MODEL OF THE SYSTEM PROVIDING INFORMATION SECURITY ON TRANSPORT

The features of the modeling system, which ensure information security at the transport management have been considered in this article. A big variety of such systems and of the information, which is processed in the information systems, were allocated as the main distinguishing factors. It is possible to research such systems, using methods of modeling different processes of their functioning. The discrete method of presenting information security processes is offered as a mathematical scheme for describing the dynamics of a system which provides information security. This method corresponds to their content and facilitates their mathematical description greatly. Evaluation of the actual state of the information security system is the most important step, which affects to the quality of decisions in the management of information security in the organization. This system of displaying helps to reveal the interdependence and mutual influence of various factors, which affect the system of providing the information security in organization. Also this system can be used as methodological basis for the development of specific techniques. Developing of a formal scheme allows you to structure and articulate the essence of the problem of the evaluation of the actual state of the information security system.

Key words: information security, the model, formalization, management, information system, evaluation.

REFERENCES

1. Smirnov, V., and E. Shaburov. *Information System Transportation Safety*. Web. 29 July 2015 <http://federalbook.ru/files/BEZOPASNOST/soderghanie/NB%20I/VIII/Smirnov.pdf>.

2. Presidential Decree of March 06, 1997 № 188 "On Approval of the List of confidential information" (as amended). Web. 29 July 2015 <http://base.garant.ru/10200083/>.

3. Federal Law of the Russian Federation of 27.07.2006 №149-FZ "On information, information technologies and information protection". Web. 29 July 2015 <http://ivo.garant.ru/#/document/12148555/paragraph/3471:2>.

4. Nyrkov, A. P., S. S. Sokolov, and A. S. Belousov. "Multiservice Network of Transportation Industry." *Vestnik komp'iuternykh i informatsionnykh tekhnologii (Herald of computer and information technologies)* 4 (2014): 33 – 38. DOI: 10.14489/vkit.2014.04.pp.033–038.

5. Nyrkov, A. P., S. S. Sokolov, E. A. Mustakaeva, and V. A. Malcev. "Providing the necessary information security regime assets multiservice network transport industry." *Information security problems. Computer systems*. 1 (2014): 47–51.

6. Nyrkov, A. P., S. S. Sokolov, and A. S. Belousov. "Algorithmic support of optimization of multicast data transmission in networks with dynamic routing." *Modern Applied Science* 9.5 (2015): 162-176. DOI: 10.5539/mas.v9n5p162.

7. Nyrkov, A. P., S. S. Sokolov, A. S. Belousov, N. M. Kovalnogova, and V. A. Malcev. "Ensuring safe operation of multiservice network in transport industry." *Proceedings of Tomsk State University of Control Systems and Radioelectronics* 2 (2014): 143–149.

8. Zapechnikov, S., N. G. Miloslavskaja, A. I. Tolstoj, D. V. Ushakov. *Information security of open systems. Vol. 1. Threats, vulnerabilities, attacks and approaches to protect*. M.: Hotline – Telecom, 2006.

9. Sokolov, S. S. "Model of threats of organization's information security". *Journal of University of Water Communications* 2 (2009): 176-180.

10. Vikhrov, N. M., Ju. F. Katorin, A. P. Nyrkov, et al. "On the safety of water transport infrastructure". *Maritime Bulletin* 4 (2014): 99–102.

11. Nyrkov, A. P., A. A. Nyrkov, S. S. Sokolov, and A. A. Shnurenko. *Securing objects of information transport industry.* SPb.: Publishing House of the Polytechnic. University Press, 2015.

12. Mishchenko, V. I., and A. K. Shilov. "Protecting information in state information systems." *Vestnik komp'iuternykh i informatsionnykh tekhnologii (Herald of computer and information technologies)* 3 (2015): 45-47. DOI: 10.14489/vkit.2015.03.pp.045–047.

13. Nyrkov, A. P., Ju. F. Katorin, S. S. Sokolov, and V. N. Ezhgurov. "Basic principles of secure information systems of automated management of transport and logistics complex." *Information security problems. Computer systems.* 2 (2013): 54–58.

14. Nyrkov, A. P., and N. Y. Vaygandt. "Data integrity control in the transport monitoring." *Journal of University of Water Communications* 1 (2013): 54-61.

15. Nyrkov, A. P., A. V. Bashmakov, and S. S. Sokolov. "Technique of designing secure information systems in transport." *Information security problems. Computer systems.* 3 (2010): 58–61.

16. Yazov, Y. K. *Fundamentals methodology quantifying the effectiveness of information security in computer systems*. Rostov-na-Donu: Publishing House of SKNC VS, 2006.

17. Horev, A. A. "Evaluating the effectiveness of the protection of assistive technology." *Special equipment*. 2 (2007): 48-60; 3 (2007): 50–63.

18. Shivdyakov, L. A., I. N. Bozarnyj, Ju. K. Jazov. "System of indicators to measure the state of information security in the automated system for monitoring results." *Information and Security.* 2 (2009): 251–257.

19. Nyrkov, A. P., and S. A. Rudakova. "The technique of audit of information objects for information security requirements." *Journal of University of Water Communications* 3 (2012): 146–149.

20. Zhigulin, G. P., A. S. Zgurskij, and A. N. Ljulchenko. "Concept, the main stages and types of information security audit in the enterprise." *Actual problems of the humanities and the natural sciences* 10 (2012): 57–60.

21. Serdyuk, V. A. "Information security audit – the basis of the effective protection of enterprise." *BYTE / Russia* 4 (2006): 32–35.

22. Makarov, A. D., D. V. Shved, and V. G. Shved. "Innovative approach in the Russian economy – the formal model of information security management." *Actual research directions: from theory to practice: the materials V Intern. scientific and practical. Conf* Cheboksary: CNS "Interactive plus", 2015: 37–42.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Люльченко Андрей Николаевич –
соискатель, генеральный директор.
ООО «РАЦ «ПРОМЭКСПЕРТ»
school@gkspr.ru
Ныркov Анатолий Павлович –
доктор технических наук, профессор.
ФГБОУ ВО «Государственный университет
морского и речного флота
имени адмирала С. О. Макарова»
kaf.koib@gmail.com
Швед Виктор Григорьевич –
доктор технических наук, доцент.
НОУ ДПО «Учебный центр «СпецПроект»
school@gkspr.ru

INFORMATION ABOUT THE AUTHORS

Lyulchenko Andrei Nikolaevich –
competitor, General director.
LLC RAC "PromEkspert"
school@gkspr.ru
Nyrkov Anatoliy Pavlovich –
Doctor of Engineering, professor.
Admiral Makarov State University
of Maritime and Inland Shipping
kaf.koib@gmail.com
Shved Viktor Grigorievich –
Doctor of Engineering, associate professor.
Private educational establishment of additional
vocational training "Training Center "SpecProject"
school@gkspr.ru