НАУЧНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОГО УПРАВЛЕНИЯ РИСКАМИ НАРУШЕНИЯ ЗАЩИЩЕННОСТИ ФУНКЦИОНАЛЬНО-ОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ[1]

***Чукляев И.И.*[2]**

В статье уточнен понятийно–терминологический аппарат управления рисками информационной безопасности. Представлено обобщенное описание разработанного метода и реализующих его моделей для комплексного управления рисками нарушения защищенности функционально–ориентированных информационных ресурсов информационно–управляющих систем. Предлагаемый подход позволяет детализировать информационно–управляющие системы относительно функциональной, информационной, организационной и технической подсистем; сформировать функционально–ориентированные информационные ресурсы, структура которых содержит многоаспектную информацию для выполнения всей совокупности задач управления информационно–управляющими системами; расширить возможности по созданию перспективных средств защиты, ориентированных на комплексную защиту выполнения задач с учетом уровней управления систем.

***Ключевые слова**: сложная организационно–техническая система, функционально–ориентированные информационные ресурсы, риск–событие, риск–ситуация нарушения защищенности.*

DOI 10.21681/2311-3456-2016-4-61-71

Введение

Интеграция информационно-телекоммуникационных технологий в информационно-управляющих системах (ИУС) актуализирует вопросы обеспечения их защищенности от несанкционированных внешних и/или внутренних воздействий дестабилизирующего характера (НСВ), заключающихся в разрушении, повреждении компонентов, модификации (искажении) данных [1, 2], ведущих к нарушению выполнения задач управления.

В настоящее время предложены разнообразные методы и средства обеспечения защищенности ИУС и циркулирующих данных в условиях НСВ. Однако, как правило, они «локализованы» относительно отдельных совокупностей данных и процессов и не ориентированы на комплексную защиту выполнения задач с учетом уровней управления ИУС и комплексное управление рисками нарушения их защищенности [1, 3].

Актуальность

Риск является неизбежным, сопутствующим фактором функционирования и развития любой сложной системы или процесса. Управление рисками представляет собой одну из основных современных концепций управления сложными организационно-техническими системами (ОТС) [1, 4].

Под понятием «риск», как правило, понимается сочетание вероятности (возможности) события (нанесения ущерба) и его негативных последствий (тяжести этого ущерба). В ряде случаев под риском также понимают вероятность (возможность) отклонения от ожидаемого результата или события. Под понятием «управление риском» понимается либо деятельность по снижению итогового ущерба для системы; либо мероприятия по страхованию от потенциального ущерба; либо устранение источников рисков; либо рекомбинация причинно-следственной связанности событий, несущих потенциальной ущерб для системы.

Использование данной концепции обосновано особенностями построения и функционирования ОТС, к которым, прежде всего, можно отнести:

- сложность структуры, многокомпонентность, многочисленные протекающие процессы, учет большого количества параметров;
- разнообразие рискообразующих системных и внешних факторов вероятностного и нестохастического характера;

1 Исследование выполнено при поддержке РФФИ в рамках научного проекта № 13-07-97518 и гранта Президента Российской Федерации № МК-3603.2014.10.

2 Чукляев Илья Игоревич, кандидат технических наук, доцент, Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М.Василевского, г. Смоленск, smolrsu@mail.ru

- динамичное изменение структуры;
- неполнота исходной информации;
- невозможность создания и использования общих аналитических моделей системы и процессов её функционирования;
- наличие сложных нелинейных зависимостей между параметрами;
- необходимость оперативного принятия управленческих решений;
- ограниченные возможности экспериментальных исследований;
- возможности по оперативному управлению в псевдореальном масштабе времени, обусловленном инерционностью системы;
- необходимость использования различных подходов к моделированию системы и использование результатов моделирования для оперативного управления системой.

Необходимо отметить, что низкая структурированность процессов обеспечения защищенности выполнения задач с учетом уровней управления ОТС в условиях рисков, их слабая формализуемость и высокая динамика изменений различного характера не позволяют в полной мере использовать существующий аппарат обеспечения защищенности ОТС. Это обстоятельство, в свою очередь, обуславливает необходимость разработки метода комплексного управления рисками нарушения защищенности ФОИР ИУС, основанного на методологиях [1, 5]:

- нечеткого моделирования, предложенной и развитой в работах таких ученых, как А.Н. Мелихов, А.Н. Борисов, В.П. Тарасик, А.И. Галушкин, А.А. Вавилов, Н.П. Бусленко, В.В. Калашников, Ю.Г. Карпов, В.Н. Волкова, А.Н. Васильев, Д.А. Тархов, С.В. Емельянов, А.И. Орлов, В.Г. Лисиенко, В.И. Капалин, Н.В. Замятина, Д.А Мокогон, А.А. Самарский, В.В. Окольнишников, А.И. Миков, Б.В. Палюх, Ю.И. Рыжиков, А.Г. Ивахненко, Е.В Бодянский, Е.И. Кучеренко, А.И. Михалев, А.А. Воронов, Б.Я. Советов, С.А. Яковлев, Ю.И. Бродский, Е.Э. Ширкова и других; зарубежных ученых – Л.А. Заде (L.A. Zadeh), Д. Дюбуа (D. Dubuis), А. Прад (H. Prade), Е. Мамдани (E. Mamdani), А. Кофман (A. Kaufmann), S. Haykin, R. Fujimoto, A. Law, R. Sargent, S. Ferenci, K. Perumalla, B. Perakath, M. McComas, J. Carson, C. Pegden, R.Bagrodia, R.Meyer, B. Zeigler, W. Kelton, J. Banks и других;
- по учету различного типа неопределенности теорий нечетких вычислений, нечетких множеств и отношений, нечеткой меры, нечеткой логики, нечеткого вывода и нечеткого моделирования, предложенных в работах А.Е. Алтунина, И.З. Батыршина, А.Н. Борисова, Л.С. Берштейна, С.Я. Коровина, О.А. Крумберга, А.Н. Мелихова, С.А. Орловского, М.В. Семухина, В.Б. Силова, Л.А. Заде (L.A. Zadeh), J.C. Bezdek, R. Bellman, J.L. Castro, H. Larsen, M. Sugeno, T. Takagi, T. Terano, Y. Tsukamoto, R. Yager и других;
- нечетких и гибридных нечетких моделей, сформулированных в исследованиях Л.Г. Комарцовой, В.В. Борисова, А.С. Федулова, Н.Г. Ярушкина, R. Fuller, Y. Hayashi, D.J. Hunt, J.–S.R. Jang, J.M. Keller, B. Kosko, R. Krishnapuram, E.T. Lee, H.–M. Lee, S.C. Lee, J.M. Mendel, S. Mitra, S. Pal, W. Pedrycz, D. Rutkowski, L. Rutkowski, C.–T. Sun, L.X. Wang и других;
- создания программных средств интеллектуальных систем, в том числе экспертных систем и систем поддержки принятия решений, основанных на работах отечественных ученых Д.А. Поспелова, А.Н. Аверкина, А.А. Башлыкова, В.Н. Вагина, В.В. Емельянова, А.П. Еремеева, Н. Г. Загоруйко, О.П. Кузнецова, В.М. Курейчика, О.И. Ларичева, А.С. Нариньяни, Г.С. Осипова, А.Б. Петровского, Г.С. Плесневича, В.Э. Попова, Г.В. Рыбиной, В.А. Смирнова, В.Б. Тарасова, В.В. Троицкого, В.К. Финна, И.Б. Фоминых, В.Ф. Хорошевского, С.В. Артюхова, О.А. Базюкина, В.Ю. Королева, А.А. Кудрявцева, В.Е. Бенинга, С.Я. Шоргин и др.; зарубежных ученых J. Allen, C. Demetresku, R. Detcher, A. Gereviny, G. Italiano, A. Krokhin, I. Meiri, L. Schubert, T. Saaty, T. Van Allen, N. Crockford, Morgan, Granger и других.

Понятийно-терминологический аппарат

Существующий понятийно-терминологический аппарат, применяемый при формализации процессов выполнения задач с учетом уровней управления и комплексного управления рисками нарушения защищенности сложных ОТС, является разобщенным, допускает различную трактовку, характеризуется слабой связанностью и требует уточнения.

Исходя из этого, информационно-управляющую систему предлагается рассматривать как функциональную, информационную, организационную и техническую подсистемы. Компоненты этих подсистем распределены по уровням управления ИУС (табл.1) [6].

Предлагаемая структура функционально-ориентированных информационных ресурсов (ФОИР) ИУС содержит многоаспектную информацию для выполнения всей совокупности задач управления ИУС и представляются в виде [6, 7]:

$$\begin{aligned} ФОИР_{ИУС} = \{ФОИР_{Ai}\} \ \triangleright\triangleleft \{IR\} \triangleright\triangleleft \\ \triangleright\triangleleft \{Функция\} \triangleright\triangleleft \{Право\} \triangleright\triangleleft \{ДЛ\} \triangleright\triangleleft \\ \triangleright\triangleleft \{Механизм\} \triangleright\triangleleft \{Взаимосвязи\} \triangleright\triangleleft \\ \triangleright\triangleleft \{Свойства\} \triangleright\triangleleft \{Временные\ параметры\}; \end{aligned} \quad (1)$$

Функционально-ориентированные информационные ресурсы для решения задач *i*-го уровня управления:

$$ФОИР_{Ai}=\{ФОИР_{Aj}\} \triangleright\triangleleft \{Вход\ _{Функция^{i}_{nm}}\} \triangleright\triangleleft \{Управление\ _{Функция^{i}_{nm}}\} \triangleright\triangleleft \{Вызов\ _{Функция^{i}_{nm}}\} \triangleright\triangleleft \{Выход\ _{Функция^{i}_{nm}}\} \triangleright\triangleleft \{Функция^{1}_{nm}\} \triangleright\triangleleft \{Право\} \triangleright\triangleleft \{ДЛ_{bc}\} \triangleright\triangleleft \{СрАвт\} \triangleright\triangleleft \{Взаимосвязи\} \triangleright\triangleleft \{Свойства\} \triangleright\triangleleft \{Временные\ параметры\};\quad (2)$$

Функционально-ориентированные информационные ресурсы для решения задач j-го уровня управления:

$$ФОИР_{Aj}=\{N_{IR}\} \triangleright\triangleleft \{Функция^{3}_{ntmkl}\} \triangleright\triangleleft \{Право\} \triangleright\triangleleft \{ДЛ_{bcd}\} \triangleright\triangleleft \{Устройства\} \triangleright\triangleleft \{Взаимосвязи\} \triangleright\triangleleft \{Свойства\} \triangleright\triangleleft \{Временные\ параметры\},\quad (3)$$

где: $\{ФОИРИУС\}$, $\{ФОИР_{Ai}\}$, $\{ФОИР_{Aj}\}$ – функционально-ориентированные информационные ресурсы ИУС соответствующих уровней управления, $\{Взаимосвязи\}$ – взаимосвязи функционально-ориентированных информационных ресурсов ИУС соответствующих уровней управления, $\{Свойства\}$ – свойства защищенности, предъявляемые к функционально-ориентированным информационным ресурсам ИУС соответствующих уровней управления, $\{Временные\ параметры\}$ – временные параметры, $\triangleright\triangleleft$ – операция агрегирования, характеризующая объединение и укрупнение показателей функционально-ориентированных информационных ресурсов ИУС соответствующих уровней управления.

Риски нарушения защищенности ФОИР ИУС предлагается рассматривать как совокупность источников риск-событий SR, риск-событий RE, риск-ситуаций RS нарушения защищенности ФОИР ИУС и взаимосвязей Con между ними (рис.1) [1, 4].

Источник риск-события нарушения защищенности ФОИР ИУС – элемент функциональной, информационной, организационной и технической подсистем ФОИР ИУС, на которые направлены угрозы применения НСВ, порождающие риск-события нарушения защищенности ФОИР ИУС.

Риск-событие нарушения защищенности ФОИР ИУС – событие, наступление которого может привести к нарушению защищенности ФОИР ИУС.

Риск-ситуация нарушения защищенности ФОИР ИУС – совокупность обусловленных причинно-следственными связями источников риск-событий и риск-событий нарушения защищенности ФОИР ИУС.

Таким образом, предлагаемый аспект рассмотрения рисков нарушения защищенности ФОИР

Таблица 1.

Пример распределения компонентов подсистем информационно-управляющей системы на смежных уровнях управления

Уровни управления ИУС	Подсистемы ИУС			
	Функциональная	**Информационная**	**Организационная**	**Техническая**
ИУС	Задачи управления <*Функция*>	Информационные потоки данных <*IR*>	Должностные лица (ДЛ) <*ДЛ*>	Техническая основа <*Механизм*>
Уровень *Ai*	Задачи управления, реализуемые ДЛ <$Функция^{1}_{nm}$>	Информационные потоки <*IR*>, <$Вход\ _{Функция^{i}_{nm}}$>, <$Управление\ _{Функция^{i}_{nm}}$>, <$Вызов\ _{Функция^{i}_{nm}}$>, <$Выход\ _{Функция^{i}_{nm}}$>	Должностные лица органов управления <$ДЛ_{bc}$>	Средства автоматизации <*СрАвт*>
Уровень *Aj*	Задачи управления, реализуемые устройствами (аппаратурой) <$Функция^{3}_{ntmkl}$>	Показатели структуры <N_{IR}> информационных потоков данных, <$Вход\ _{Функция^{3}_{ntmkl}}$>, <$Управление\ _{Функция^{3}_{ntmkl}}$>, <$Вызов\ _{Функция^{3}_{ntmkl}}$>, <$Выход\ _{Функция^{3}_{ntmkl}}$>	Действия ДЛ <$ДЛ_{bcd}$>	Устройства (аппаратура) <*Устройства*>

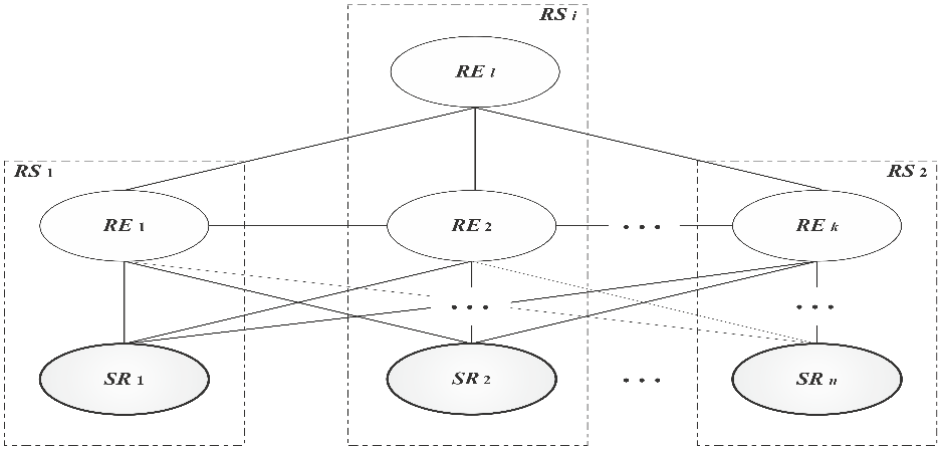

***Рис.1**. Графическое представление источников риск-событий SR, риск-событий RE и риск-ситуаций RS нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющей системы*

ИУС детализируется понятиями «источник риск-события», «риск-событие» и «риск-ситуация» нарушения защищенности ФОИР ИУС. Данное уточнение позволяет дифференцировано охарактеризовать как причины возникновения рисков, в том числе и единичного, последствия, так и мероприятия, направленные на устранение результатов возникновения рисков нарушения защищенности ФОИР ИУС, а также принадлежность традиционно «приписываемых» характеристик к следующим понятиям:

«риск» – характеристика «уровень риска»;

«событие», характеризующее риск нарушения защищенности, – характеристиками «существенность», «категория» и «приемлемость»;

«мероприятие», направленное на устранение результатов реализации событий нарушения защищенности, – «уровень последствия».

Постановка задачи

Для разработки метода комплексного управления рисками нарушения защищенности ФОИР ИУС требуется:

- уточнить понятийно-терминологический аппарат;
- исследовать процессы, способы и модели управления рисками, а также обосновать возможности их применения относительно этапов управления рисками нарушения защищенности ФОИР ИУС;
- выполнить анализ условий и способов учета неопределенности при комплексном управлении рисками;
- сформировать требования к нечетким моделям комплексного управления рисками нарушения защищенности ФОИР ИУС;
- разработать нечеткие модели комплексного управления рисками нарушения защищенности ФОИР ИУС;
- разработать алгоритмы построения и применения нечетких моделей комплексного управления рисками нарушения защищенности ФОИР ИУС;
- выработать рекомендации по комплексному управлению рисками нарушения защищенности ФОИР ИУС.

Формализованное описание комплексного управления рисками нарушения защищенности ФОИР ИУС представляется в виде [1, 4, 8]:

$$Z_{ФОИР\ ИУС}(Q_k,\ V_k) \xrightarrow{\tilde{P}_k} V_k \max; \quad (4)$$

$$Risk_{ФОИР\ ИУС} = f(Z_{ФОИР\ ИУС}), \quad (5)$$

где: $Z_{ФОИР\ ИУС}$ – защищенность функции управления верхнего уровня функционально-ориентированных информационных ресурсов ИУС, Q_k – смешанные оптимальные стратегии угроз применения НСВ нарушения защищенности функционально-ориентированных информационных ресурсов ИУС, V_k – оптимальный риск нарушения защищенности функционально-ориентированных информационных ресурсов ИУС при взаимном применении сторонами смешанных оптимальных стратегий (P_k и Q_k), $\tilde{P}_k$ – классы мероприятий (оптимальные смешанные стратегии) управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов ИУС, $Risk_{ФОИР\ ИУС}$ – риск нарушения защищенности функции управления верхнего уровня функционально-ориентированных информационных ресурсов ИУС.

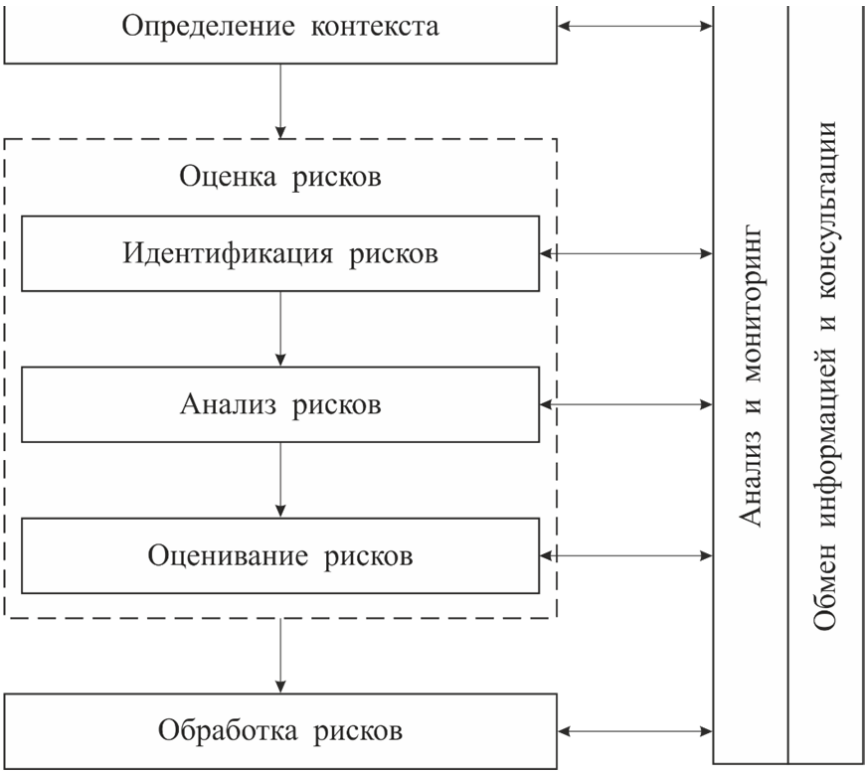

***Рис.2**. Графическое представление процессов управления рисками*

Гибридная нечеткая модель комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем

Процессы управления рисками (рис.2) регламентированы руководящими документами [1, 4] и определяют реализацию следующих этапов (подпроцессов):

- анализ и мониторинг;
- обмен информацией и консультации;
- управление рисками: определение контекста, оценка рисков (идентификация рисков, анализ рисков, оценивание рисков) и обработка рисков.

Разработанный метод комплексного управления рисками нарушения защищенности ФОИР ИУС основан на гибридной нечеткой модели комплексного управления рисками нарушения защищенности ФОИР ИУС.

На рис.3 представлена диаграмма, иллюстрирующая взаимосвязи созданной нечеткой гибридной модели комплексного управления рисками нарушения защищенности ФОИР ИУС и структуры составляющих ее нечетких моделей (рис.4), направленных на реализацию метода комплексного управления рисками нарушения защищенности ФОИР ИУС [1, 4].

Формализованное описание гибридной нечеткой модели комплексного управления рисками нарушения защищенности ФОИР ИУС представляется в виде [1, 4]:

$$\begin{cases} SR,\ RE,\ RS,\ Con \\ Risk_{SR},\ Risk_{RE},\ Risk_{RS},\ Con,\ Oper \\ A_k,\ a_{ij}^k,\ p_m^k,\ q_m^k,\ P_k,\ Q_k,\ \alpha,\ \beta,\ V_k \\ V_k,\ P_k \end{cases} \rightarrow q_m^k,\ Q_k,\ \tilde{P}_k, \quad (6)$$

где: $Risk_{SR}$, $Risk_{RE}$, $Risk_{RS}$ – значения рисков источников риск-событий, риск-событий и риск-ситуаций ФОИР ИУС, $Oper$ – логические T-операции t-нормы («**И**») или min-конъюнкции между источниками риск-событий и риск-событиями нарушения защищенности ФОИР ИУС, A_k – матрица рисков нарушения защищенности ФОИР ИУС, a_{ij}^k – элементы матрицы рисков Ak нарушения защищенности ФОИР ИУС, p_m^k – чистые стратегии применения мероприятий управления рисками нарушения защищенности ФОИР ИУС, q_m^k – чистые стратегии угроз применения НСВ нарушения защищенности ФОИР ИУС, α – допустимые значения уровней рисков нарушения защищенности ФОИР ИУС, β – критические β значения уровней рисков нарушения защищенности ФОИР ИУС.

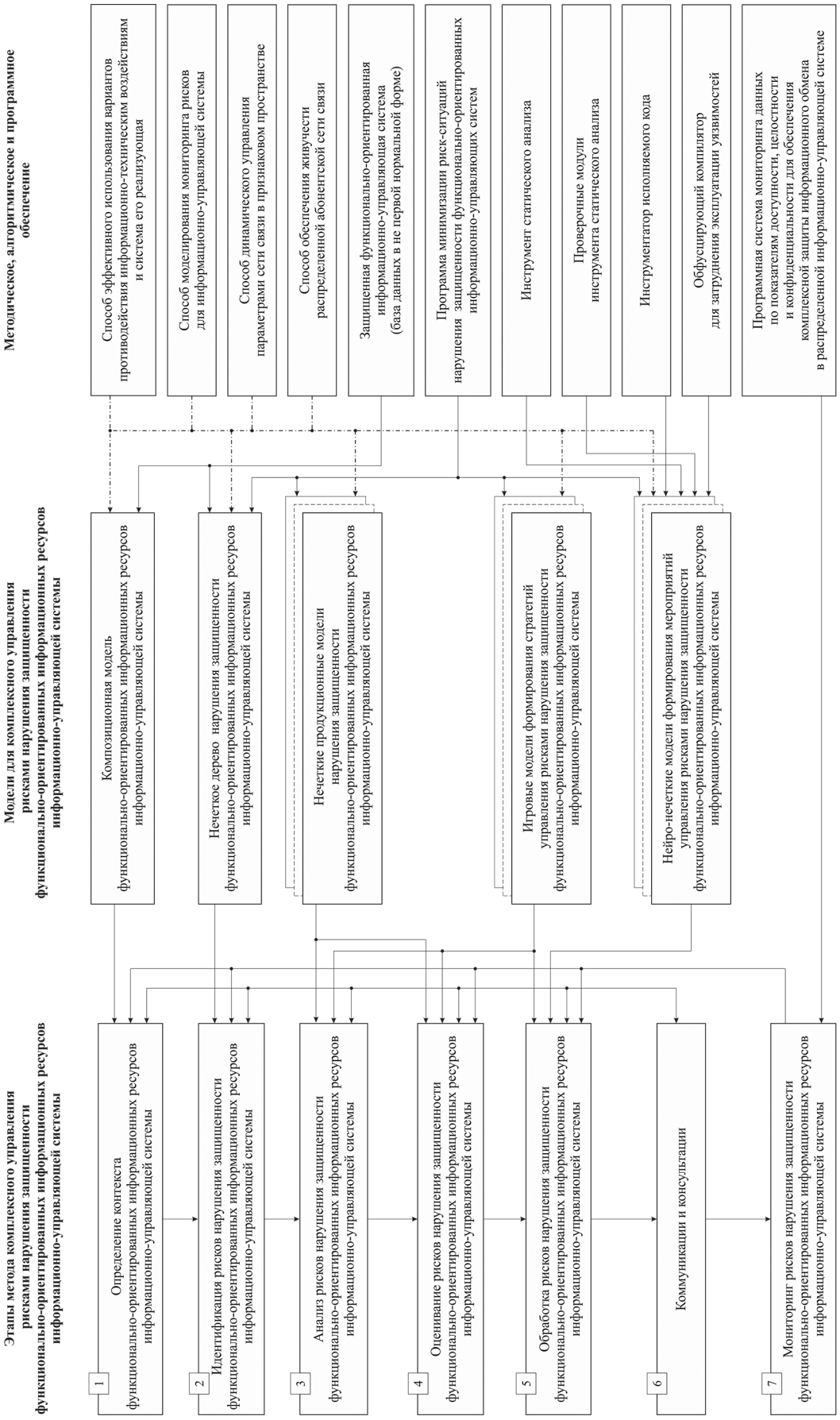

***Рис. 3**. Метод, модели и методическое, алгоритмическое, программное обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющей системы*

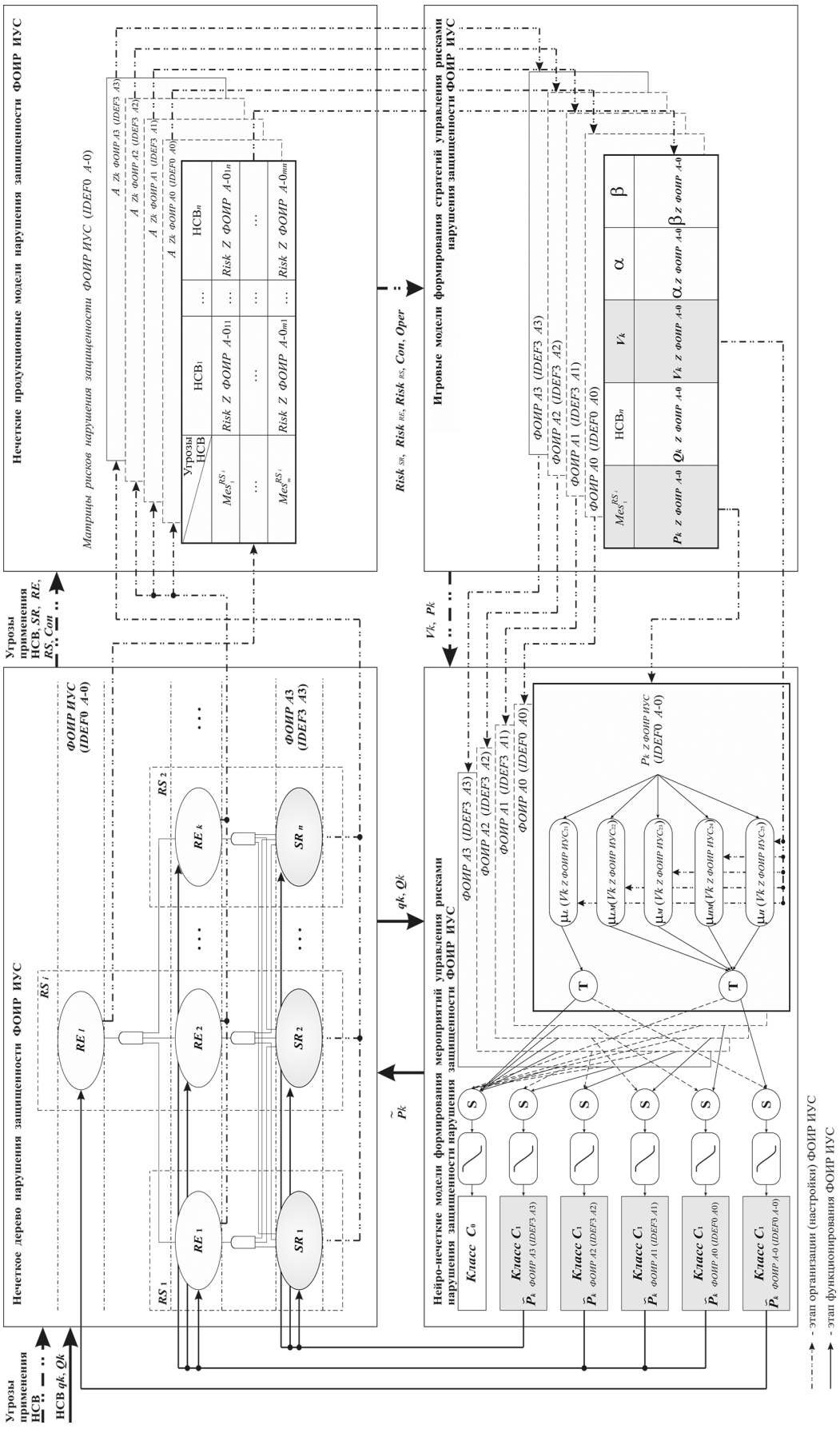

Рис. 4. *Структура нечеткой гибридной модели комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющей системы*

Этап 1. Определение контекста ФОИР ИУС.

На основе получаемой информации о составе и топологии ИУС; подсистемах, уровнях управления, структуре и взаимосвязях показателей ФОИР ИУС и защищенных ФОИР ИУС; базисных схемах взаимодействия ФОИР ИУС; операциях манипулирования и обработки функционального комплекса данных ФОИР ИУС, а также рисках нарушения защищенности ФОИР ИУС и угрозах применения НСВ; ограничениях на управление рисками нарушения защищенности ФОИР ИУС; статистической информации выполняется уточнение и обобщение указанной информации.

Этап 2. Идентификация рисков нарушения защищенности ФОИР ИУС.

Информация, полученная на предыдущем этапе; угрозы применения НСВ на подсистемы уровней управления ФОИР ИУС; риски (источники риск-событий, риск-события и риск-ситуации) нарушения защищенности ФОИР ИУС; ограничения на управление рисками нарушения защищенности ФОИР ИУС являются исходными для:

- определения направленности угроз применения НСВ;

- формирования нечеткого дерева нарушения защищенности ФОИР ИУС $FTIS$, которое включает источники риск-событий SR, риск-события RE и риск-ситуации RS, и взаимосвязи Con нарушения защищенности ФОИР ИУС;

- определения критериев управления рисками нарушения защищенности ФОИР ИУС.

Этап 3. Анализ рисков нарушения защищенности ФОИР ИУС.

В соответствии с критериями управления рисками нарушения защищенности ФОИР ИУС и сведениями о результатах мониторинга нечеткого дерева нарушения защищенности ФОИР ИУС уточняются угрозы применения НСВ; структура и взаимосвязи между компонентами нечеткого дерева нарушения защищенности ФОИР ИУС.

Этап 4. Оценивание рисков нарушения защищенности ФОИР ИУС.

Нечеткими продукционными моделями нарушения защищенности ФОИР ИУС $RBFM$ определяются значения рисков (источников риск-событий $Risk_{SR}$, риск-событий $Risk_{RE}$ и риск-ситуаций $Risk_{RS}$) нечеткого дерева нарушения защищенности ФОИР ИУС.

Оценка значений возникновения рисков нарушения защищенности ФОИР ИУС проводится с применением операций агрегирования $Oper$ логическими T-операциями t-нормы («**И**», min-конъюнкция).

Этап 5. Обработка рисков нарушения защищенности ФОИР ИУС (этап организации (настройки) ФОИР ИУС).

Обработка рисков нарушения защищенности ФОИР ИУС выполняется игровыми моделями формирования стратегий управления рисками нарушения защищенности ФОИР ИУС $MSGMF$ [9]. Исходными данными для данного этапа являются информация, полученная на предыдущих этапах, а также мероприятия управления рисками нарушения защищенности ФОИР ИУС. Выходной информацией данного этапа является:

Матрицы A_k рисков нарушения защищенности подсистем уровней управления ФОИР ИУС;

- мероприятия и чистые стратегии p_m^k применения мероприятий, классы мероприятий (смешанные оптимальные стратегии) P_k управления рисками нарушения защищенности ФОИР ИУС;

- угрозы и чистые стратегии q_m^k применения НСВ, классы угроз (смешанные оптимальные стратегии) применения Q_k нарушения защищенности ФОИР ИУС;

- оптимальные риски V_k нарушения защищенности ФОИР ИУС при взаимном применении сторонами смешанных оптимальных стратегий (P_k и Q_k);

- допустимые α уровни рисков нарушения защищенности ФОИР ИУС;

- критические β уровни рисков нарушения защищенности ФОИР ИУС.

- уточненные ограничения на управление рисками нарушения защищенности ФОИР ИУС.

Этап 6. Обработка рисков нарушения защищенности ФОИР ИУС (этап функционирования ФОИР ИУС).

Реализация данного этапа выполняется нейро-нечеткими моделями формирования мероприятий управления рисками нарушения защищенности ФОИР ИУС NFC и заключается в выработке классов мероприятий (смешанных оптимальных стратегий) $\widetilde{P}_k$ управления рисками нарушения защищенности ФОИР ИУС в интересах обеспечения оптимальных значений рисков V_k нарушения защищенности ФОИР ИУС при реализации НСВ (смешанных оптимальных стратегий) Q_k [10-15].

Выработка классов мероприятий (смешанных оптимальных стратегий) $\widetilde{P}_k$ управления рисками нарушения защищенности ФОИР ИУС выполняется нейро-нечеткими классификаторами нейро-нечетких моделей. Их обучение выполняется разработанным алгоритмом обучения, который позволяет выполнить их настройку антагонистическими смешанными стратегическими играми

в матричной постановке посредством игровых моделей формирования стратегий управления рисками нарушения защищенности ФОИР ИУС на этапе организации (настройки) ФОИР ИУС.

Этапы «Коммуникации и консультации» и «Мониторинг рисков нарушения защищенности ФОИР ИУС» предназначены для мониторинга и обмена данными, а также сведениями о необходимых изменениях в применяемых нечетких моделях.

Выводы

Метод комплексного управления рисками нарушения защищенности ФОИР ИУС, основанный на гибридной нечеткой модели комплексного управления рисками нарушения защищенности ФОИР ИУС, в отличие от существующих позволяет:

- реализовать процессы комплексного управления рисками нарушения защищенности ФОИР ИУС;
- учитывать условия как стохастической, так и нестохастической неопределенности и системы предпочтений, задающих формализованные мнения экспертов о зависимостях выходных переменных от входных, а также влияния рисков нарушения защищенности подсистем уровней управления ФОИР ИУС на функцию управления верхнего уровня ФОИР ИУС;
- гибко и оперативно адаптироваться под изменяющиеся условия управления рисками нарушения защищенности ФОИР ИУС;
- компактно представлять сведения о рисках нарушения защищенности ФОИР ИУС на основе предлагаемых понятий «источник риск-события», «риск-событие» и «риск-ситуация» нарушения защищенности ФОИР ИУС;
- выполнять дифференцированный анализ нарушений защищенности подсистем уровней управления ФОИР ИУС относительно угроз применения НСВ и рисков нарушения защищенности ФОИР ИУС;
- учитывать риски нарушения защищенности подсистем уровней управления ФОИР ИУС и вырабатываемые мероприятия управления рисками нарушения защищенности ФОИР ИУС;
- формировать мероприятия (смешанные оптимальные стратегии) управления рисками нарушения защищенности ФОИР ИУС на основе спрогнозированных смешанных оптимальных стратегий угроз применения НСВ;
- определять и обеспечивать значения допустимых и критических уровней рисков, а также оптимальных рисков нарушения защищенности ФОИР ИУС посредством вырабатываемых классов мероприятий (смешанных оптимальных стратегий) управления рисками нарушения защищенности ФОИР ИУС в условиях применения угроз НСВ;
- вырабатывать классы мероприятий (смешанные оптимальные стратегии) управления рисками нарушения защищенности ФОИР ИУС;

обеспечивать непрерывность границы между классами мероприятий управления рисками нарушения защищенности ФОИР ИУС.

Предлагаемые метод и модели комплексного управления рисками нарушения защищенности ФОИР ИУС обеспечивают расширенные возможности по созданию перспективных средств защиты, ориентированных на комплексную защиту выполнения задач с учетом уровней управления ОТС.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э.Баумана, г. Москва, v.tsirlov@bmstu.ru*

Литература

1. Чукляев И.И. Метод и модели комплексного управления рисками нарушения защищенности информационно-управляющих систем. Монография. Смоленск: ВА ВПВО ВС РФ. 2015. 141 с.
2. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.
3. Чукляев И.И. Теоретическое обобщение предметной области «информационная безопасность». Тенденции развития методов и средств // Научно-технический сборник АО «Концерн «Системпром». № 1(6)-2015, 2015. С. 471-486.
4. Чукляев И.И. Управление рисками защищенности распределенных информационно-вычислительных систем // Системы компьютерной математики и их приложения. 2015. № 16. С. 110-112.
5. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. Монография. М: Горячая линия - Телеком, 2012. 284 с.
6. Чукляев И.И. Функционально-ориентированные ресурсы. База данных информационно-управляющей системы. Монография. Смоленск: ВА ВПВО ВС РФ. 2015. 114 с.
7. Чукляев И.И. Композиционная модель и способ построения функционально-ориентированных информационных ресурсов информационно-управляющих систем // Труды Института системного программирования РАН, том 28, вып. 2, 2016, с. 259-270. DOI: 10.15514/ISPRAS-2016-28(2)-17

8. Чукляев И.И. Система комплексной защиты функционально-ориентированных информационных ресурсов информационно-управляющих систем // Системы компьютерной математики и их приложения. 2016. № 17. С. 85-88.
9. Чукляев И.И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 2. С. 64-68.
10. Чукляев И.И. Нечеткая оценка взаимосвязей системных факторов информационно-управляющей системы в интересах повышения защищенности информационных ресурсов // Системы управления, связи и безопасности. 2015. № 1. С. 4-15.
11. Чукляев И.И. Методика построения и нечеткая модель оценки защищенности и выбора классов мероприятий по минимизации рисков на основе нейронечеткого классификатора // Известия Смоленского государственного университета. 2015. № 2-1. С. 312-319.
12. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.
13. Чукляев И.И. Анализ уязвимостей в исходных кодах программного обеспечения статическими и динамическими методами. В сборнике: XII всероссийское совещание по проблемам управления ВСПУ-2014 Институт проблем управления им. В.А. Трапезникова РАН. 2014. С. 9232-9242.
14. Чукляев И.И. Оценка уязвимостей программного обеспечения информационно-управляющих систем различного назначения методами обратной инженерии. В сборнике: Кибернетика и высокие технологии XXI века XV Международная научно-техническая конференция. НПФ «САКВОЕЕ» ООО. 2014. С. 230-237.
15. Бутусов И.В., Нащекин П.А., Романов А.А. Теоретико-семантические аспекты организации комплексной системы защиты информационных систем // Вопросы кибербезопасности. 2016. № 1 (14). С. 9-16.

METHODICAL PROVIDING COMPLEX MANAGEMENT OF RISKS OF INFORMATIONAL SECURITY OF FUNCTION-ORIENTED INFORMATION RESOURCES MANAGEMENT INFORMATION SYSTEMS

Chucklyaev I.[3]

In article the conceptual framework of risk management of information security is specified. The description of the developed method and models realizing it for complex management of risks of informational security of function-oriented information resources of management information systems is provided. The developed methodical approach allows to detail management information systems of rather functional, information, organizational and technical subsystems and to create function-oriented information resources which structure contains multiaspect information for execution of set of tasks of control of management information systems.

Keywords*: organizational and technical system, function-oriented information resources, risk management of information security.*

Reference

1. Chuklyaev I.I. Metod i modeli kompleksnogo upravleniya riskami narusheniya zashchishchennosti informatsionno-upravlyayushchikh sistem. Monografiya. Smolensk: VA VPVO VS RF. 2015. 141 P.
2. Makarenko S.I., Chuklyaev I.I. Terminologicheskiy bazis v oblasti informatsionnogo protivoborstva, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. No 1 (2), pp. 13-21.
3. Chuklyaev I.I. Teoreticheskoe obobshchenie predmetnoy oblasti «informatsionnaya bezopasnost'». Tendentsii razvitiya metodov i sredstv, Nauchno-tekhnicheskiy sbornik AO «Kontsern «Sistemprom». No 1(6)-2015, 2015, pp. 471-486.
4. Chuklyaev I.I. Upravlenie riskami zashchishchennosti raspredelennykh informatsionno-vychislitel'nykh system, Sistemy komp'yuternoy matematiki i ikh prilozheniya. 2015. No 16, pp. 110-112.

3 Ilya Chucklyaev, Ph.D., Associate Professor, Marshal of the Soviet Union A.M.Vasilevsky Army Air Defense Military Academy, Smolensk, smolarm@pochta.ru

5. Borisov V.V., Kruglov V.V., Fedulov A.S. Nechetkie modeli i seti. Monografiya. M: Goryachaya liniya - Telekom, 2012. 284 P.
6. Chuklyaev I.I. Funktsional'no-orientirovannye resursy. Baza dannykh informatsionno-upravlyayushchey sistemy. Monografiya. Smolensk: VA VPVO VS RF. 2015. 114 P.
7. Chuklyaev I.I. Kompozitsionnaya model' i sposob postroeniya funktsional'no-orientirovannykh informatsionnykh resursov informatsionno-upravlyayushchikh system, Trudy Instituta sistemnogo programmirovaniya RAN, tom 28, vyp. 2, 2016, pp. 259-270. DOI: 10.15514/ISPRAS-2016-28(2)-17
8. Chuklyaev I.I. Sistema kompleksnoy zashchity funktsional'no-orientirovannykh informatsionnykh resursov informatsionno-upravlyayushchikh system, Sistemy komp'yuternoy matematiki i ikh prilozheniya. 2016. No 17, pp. 85-88.
9. Chuklyaev I.I. Igrovaya model' obosnovaniya primeneniya sredstv kompleksnoy zashchity informatsionnykh resursov ierarkhicheskoy informatsionno-upravlyayushchey sistemy, T-Comm: Telekommunikatsii i transport. 2015. T. 9. No 2, pp. 64-68.
10. Chuklyaev I.I. Nechetkaya otsenka vzaimosvyazey sistemnykh faktorov informatsionno-upravlyayushchey sistemy v interesakh povysheniya zashchishchennosti informatsionnykh resursov, Sistemy upravleniya, svyazi i bezopasnosti. 2015. No 1, pp. 4-15.
11. Chuklyaev I.I. Metodika postroeniya i nechetkaya model' otsenki zashchishchennosti i vybora klassov meropriyatiy po minimizatsii riskov na osnove neyronechetkogo klassifikatora, Izvestiya Smolenskogo gosudarstvennogo universiteta. 2015. No 2-1, pp. 312-319.
12. Avetisyan A.I., Belevantsev A.A., Chuklyaev I.I. Tekhnologii staticheskogo i dinamicheskogo analiza uyazvimostey programmnogo obespecheniya, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. No 3 (4), pp. 20-28.
13. Chuklyaev I.I. Analiz uyazvimostey v iskhodnykh kodakh programmnogo obespecheniya staticheskimi i dinamicheskimi metodami. V sbornike: XII vserossiyskoe soveshchanie po problemam upravleniya VSPU-2014 Institut problem upravleniya im. V.A. Trapeznikova RAN. 2014, pp. 9232-9242.
14. Chuklyaev I.I. Otsenka uyazvimostey programmnogo obespecheniya informatsionno-upravlyayushchikh sistem razlichnogo naznacheniya metodami obratnoy inzhenerii. V sbornike: Kibernetika i vysokie tekhnologii XXI veka XV Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya. NPF «SAKVOEE» OOO. 2014, pp. 230-237.
15. Butusov I.V., Nashchekin P.A., Romanov A.A. Teoretiko-semanticheskie aspekty organizatsii kompleksnoy sistemy zashchity informatsionnykh system, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2016. no 1 (14), pp. 9-16.