УДК 004.056

Логическая модель деятельности по комплексному техническому диагностированию информационной безопасности организаций и значимых объектов критической информационной инфраструктуры

Забегалин Е. В.

Актуальность задачи: *Доктрина информационной безопасности Российской Федерации (Доктрина ИБ) использует системный подход к анализу и обеспечению информационной безопасности страны. Этот подход состоит в рассмотрении ИБ страны как безопасности её информационной сферы, которая имеет сложную структуру, раскрываемую в Доктрине ИБ. Автор статьи полагает целесообразной и актуальной задачу логического проецирования данного системного подхода Доктрины ИБ с верхнего иерархического уровня страны на другие её иерархические уровни, в том числе на уровень организаций и значимых объектов критической информационной инфраструктуры, в целях эффективной практической реализации положений Доктрины ИБ. Такое логическое проецирование должно начинаться с определения понятия информационной сферы (инфосферы) организации / объекта критической информационной инфраструктуры (Орг/ОбКИИ) и завершаться определением типового комплекса мер обеспечения безопасности инфосферы Орг/ОбКИИ, который полностью адекватен сложной структуре инфосферы и множеству угроз её безопасности.* ***Целью работы*** *является расширение стандартной логической модели корпоративной системы менеджмента информационной безопасности (СМИБ) путём добавления в эту модель комплексного технического диагностирования защищённости информационной сферы Орг/ОбКИИ. Это диагностирование должно включать процесс технического тестирования защищённости инфосферы опасными информационно-техническими воздействиями (ИТВ), которое рассматривается российскими специалистами в научных публикациях.* ***Метод решения задачи:*** *сначала, исходя из понятия информационной сферы страны, определяемого в Доктрине ИБ, разрабатывается понятие инфосферы Орг/ОбКИИ и систематизируются типовые угрозы её безопасности, а также систематизируются соответствующие им виды защитных мероприятий; потом в рамках рекомендаций стандартов по построению СМИБ разрабатывается расширенная логическая модель комплекса мероприятий по обеспечению информационной безопасности Орг/ОбКИИ как безопасности инфосферы Орг/ОбКИИ; а затем, опираясь на известные идеи российских специалистов по применению ИТВ для технического тестирования защищённости ОбКИИ, разрабатывается логическая модель комплексного технического диагностирования информационной безопасности Орг/ОбКИИ, при этом используются нотации логико-графического моделирования «Value-added Chain Diagram», «Idef0», нотация семантических сетей.* ***Новизна решения*** *заключается в содержательной разработке понятия «информационная сфера организации / объекта критической информационной инфраструктуры» и в разработке логической модели возможного комплексного технического диагностирования информационной безопасности (защищённости инфосферы) Орг/ОбКИИ, которая расширяет стандартную логическую модель корпоративной СМИБ.* ***Теоретическая значимость работы*** *состоит в логическом проецировании доктринального понятия информационной сферы страны на уровень организаций и значимых объектов критической информационной инфраструктуры, а также в логическом моделировании возможного комплексного технического диагностирования информационной безопасности (защищённости инфосферы) Орг/ОбКИИ.*

Библиографическая ссылка на статью:
Забегалин Е. В. Логическая модель деятельности по комплексному техническому диагностированию информационной безопасности организаций и значимых объектов критической информационной инфраструктуры // Системы управления, связи и безопасности. 2019. № 3. С. 145-178. DOI: 10.24411/2410-9916-2019-10308.

Reference for citation:
Zabegalin E. V. The logical model of integrated technical diagnostics of information security of organizations and significant objects of critical information infrastructure. *Systems of Control, Communication and Security*, 2019, no. 3, pp. 145-178. DOI: 10.24411/2410-9916-2019-10308 (in Russian).

Ключевые слова: *информационная безопасность, информационная сфера, инфосфера, техническое диагностирование, техническое тестирование, информационно-техническое воздействие, логическая модель.*

Актуальность и постановка задачи

Доктрина информационной безопасности Российской Федерации [1] (далее – *Доктрина ИБ*) проводит системный подход к анализу и обеспечению информационной безопасности России, состоящий в *рассмотрении информационной безопасности страны как безопасности её информационной сферы*.

Термин «информационная сфера» страны определён в тексте Доктрины ИБ как совокупность информации, объектов информатизации, сайтов в сети «Интернет», сетей связи, информационных технологий (ИТ), субъектов, деятельность которых связана с формированием и обработкой информации, с развитием и использованием указанных технологий, с обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

В Доктрине ИБ можно выделить следующие наиболее существенные аспекты обеспечения информационной безопасности страны, согласующиеся со структурой её информационной сферы:

- защита государственной тайны;
- защита информации в технических системах от технических разведок и от вредоносных информационно-технических воздействий (ИТВ);
- защита сознания людей от информационно-психологических воздействий (ИПВ);
- достижение независимости России от зарубежных ИТ;
- совершенствование механизмов государственного регулирования ИБ.

Полнота реализации положений Доктрины ИБ должна быть достигнута на всех иерархических уровнях государства, экономики и общества. Поэтому видится актуальным логическое проецирование системного подхода Доктрины ИБ к анализу и обеспечению информационной безопасности России с общего верхнего уровня страны на более низкие её иерархические уровни.

Не трудно представить себе схему проецирования положений Доктрины ИБ на региональный и муниципальный уровни управления путём замены её терминов и формулировок на им подобные для этих уровней управления.

Сложнее выполнить проецирование положений Доктрины ИБ на уровень организаций и значимых объектов критической информационной инфраструктуры (КИИ).

В последнем случае содержательные решения могут быть получены на основе рекомендаций отечественных и международных стандартов по организации корпоративного менеджмента ИБ. Эти стандартные рекомендации нужно дополнить такими современными аспектами ИБ, содержащимися в Доктрине ИБ, как:

- определение понятия информационной сферы применительно к организациям и значимым объектам КИИ;

- включение в систему корпоративного менеджмента ИБ мероприятий по противодействию ИПВ на персонал.

Эти дополнения могут включаться в документы корпоративных политик ИБ, содержащих своды ключевых принципов менеджмента информационной безопасности организации.

К действующим стандартам менеджмента ИБ относятся прежде всего стандарты [2-13]. Международные англоязычные стандарты [8-13] содержат новейшие версии рекомендаций, заменяющие предыдущие версии этих рекомендаций, которые продолжают действовать в России в виде ГОСТов [2-7].

Одновременно с обозначенными выше доктринальными аспектами ИБ – определения информационной сферы и потребности общества в защите от ИПВ – в ряде научных работ показана необходимость стендового тестировании защищённости информационных и коммуникационных систем тестовыми ИТВ, которая объективно обусловлена тем, что неприемлемо подвергать тестовым ИТВ поражающего действия реально функционирующие системы (особенно в критической информационной инфраструктуре страны), но можно проводить такое тестирование на натурных моделях этих систем на специальных стендах (на стендовых полигонах). Так, например:

- в статьях [14, 15] предложена структура стендового полигона оценки уровня защищенности и устойчивости функционирования критически важных информационных объектов в условиях компьютерных атак;
- в статье [16] показана необходимость стендового полигона испытаний информационно-телекоммуникационных систем ракетных комплексов стратегического назначения;
- в статье [17] описывается идея технического тестирования устойчивости компьютерных и коммуникационных компонентов робототехнических комплексов к воздействию на них сверхкороткоимпульсным электромагнитным излучением;
- в статье [18] предложен порядок экспериментальных исследований (испытаний) комплексов с беспилотными летательными аппаратами в условиях ИТВ;
- в монографии [19] достаточно подробно рассмотрены состав и классификации возможных способов технического тестирования защищённости объектов КИИ с применением средств технической и компьютерной разведок, а также с применением атакующих ИТВ.

Кроме того, требования ФСТЭК России по обеспечению безопасности значимых объектов КИИ [20] предусматривают макетирование и использование тестовых сред для тестирования систем безопасности этих объектов на стадии их проектирования.

Данные идеи, а также определяемые Доктриной ИБ сложная структура информационной сферы и комплексный состав различных мер обеспечения её безопасности, позволяют рассмотреть новую возможную меру – *«Комплексное техническое диагностирование информационной безопасности (защищённости информационной сферы)»* организации / объекта критической информационной инфраструктуры (далее – *Орг/ОбКИИ*).

Соответственно может быть поставлена актуальная теоретическая задача расширения стандартной логической модели корпоративной системы менеджмента информационной безопасности (СМИБ) с добавлением в эту модель следующих новых компонентов:

- понятия информационной сферы (далее – *инфосферы*) для Орг/ОбКИИ;
- логической модели комплекса типовых мероприятий по обеспечению безопасности инфосферы Орг/ОбКИИ с включением в эту модель возможной деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ;
- логической модели деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ с определением функциональной структуры этой деятельности.

В таких рамках постановка задачи статьи формулируется следующим образом:

- сначала, опираясь на понятие информационной сферы страны, данное в Доктрине ИБ, разработать определение понятия инфосферы организации /объекта критической информационной инфраструктуры и систематизировать типовые угрозы безопасности инфосферы Орг/ОбКИИ и соответствующие им виды защитных мероприятий;
- потом разработать логическую модель комплекса мероприятий по обеспечению безопасности инфосферы Орг/ОбКИИ в рамках стандартных рекомендаций по построению корпоративных СМИБ, в которую добавить блок деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ;
- затем разработать логическую модель деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ, раскрывающую функциональную структуру этой деятельности;
- в завершение определить новые научно-технические задачи, которые могут возникнуть и решаться в интересах практической реализации логической модели деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ.

Логическим моделированием в статье является определение специальных терминов и их содержательный логико-графический анализ на схемах.

Следующие разделы статьи последовательно представляют решение этих четырёх подзадач.

Определение понятия информационной сферы организации / значимого объекта критической информационной инфраструктуры

Логически проецируя понятие информационной сферы страны, которое определено в Доктрине ИБ, на уровень отдельных организаций и значимых объектов КИИ, можно составить следующее определение понятия информационной сферы Орг/ОбКИИ.

Информационная сфера (инфосфера) организации / объекта критической информационной инфраструктуры – агрегированная часть структуры и процессов функционирования Орг/ОбКИИ, в состав которой входят:

1) ценная информация по профилю деятельности/функционирования Орг/ОбКИИ;
2) организационная структура и документированные правила производства, обработки, приёма, передачи, распространения, потребления, хранения ценной информации;
3) технические средства производства, записи, распространения аудио и видео информации;
4) информационно-технологическая инфраструктура (ИТ-инфраструктура) в составе из средств вычислительной техники (СВТ), каналов связи (КС), обеспечивающих инженерных систем (электропитания, кондиционирования, пожаротушения и пр.);
5) прикладное программное обеспечение (ПО) производства, обработки, приёма, передачи, распространения, потребления, хранения ценной информации;
6) организационная структура и документированные правила защиты ценной информации, прикладного ПО и ИТ-инфраструктуры;
7) специальные технологические средства защиты ценной информации, прикладного ПО и ИТ-инфраструктуры;
8) действующие процессы производства, обработки, приёма, передачи, распространения, потребления, хранения ценной информации;
9) действующие процессы защиты ценной информации, прикладного ПО и ИТ-инфраструктуры;
10) сознание персонала, работающего с ценной информацией, с прикладным ПО и с ИТ-инфраструктурой, в том числе сознание администраторов автоматизированных систем (АС);
11) сознание персонала, работающего в процессах и с технологическими средствами защиты ценной информации, прикладного ПО и ИТ-инфраструктуры – сознание администраторов ИБ;
12) организационная структура и документированные правила защиты сознания персонала от информационно-психологических воздействий, побуждающих людей к нарушениям установленных правил и действующих процессов функционирования Орг/ОбКИИ, в том числе побуждающих к нарушениям безопасности ценной информации, прикладного ПО и ИТ-инфраструктуры;
13) специальные средства защиты сознания персонала от ИПВ;
14) действующие процессы защиты сознания персонала от ИПВ.

Данное определение инфосферы иллюстрирует рис. 1.

Накопленные в обществе специальные знания об ИБ, зафиксированные во множестве научных, нормативных и учебных источников, позволяют обобщить и систематизировать множество возможных типовых угроз для безопасности инфосферы Орг/ОбКИИ и соответствующие им виды защитных мероприятий. Типовой состав этих угроз в наглядном представлении показан на рис. 2.

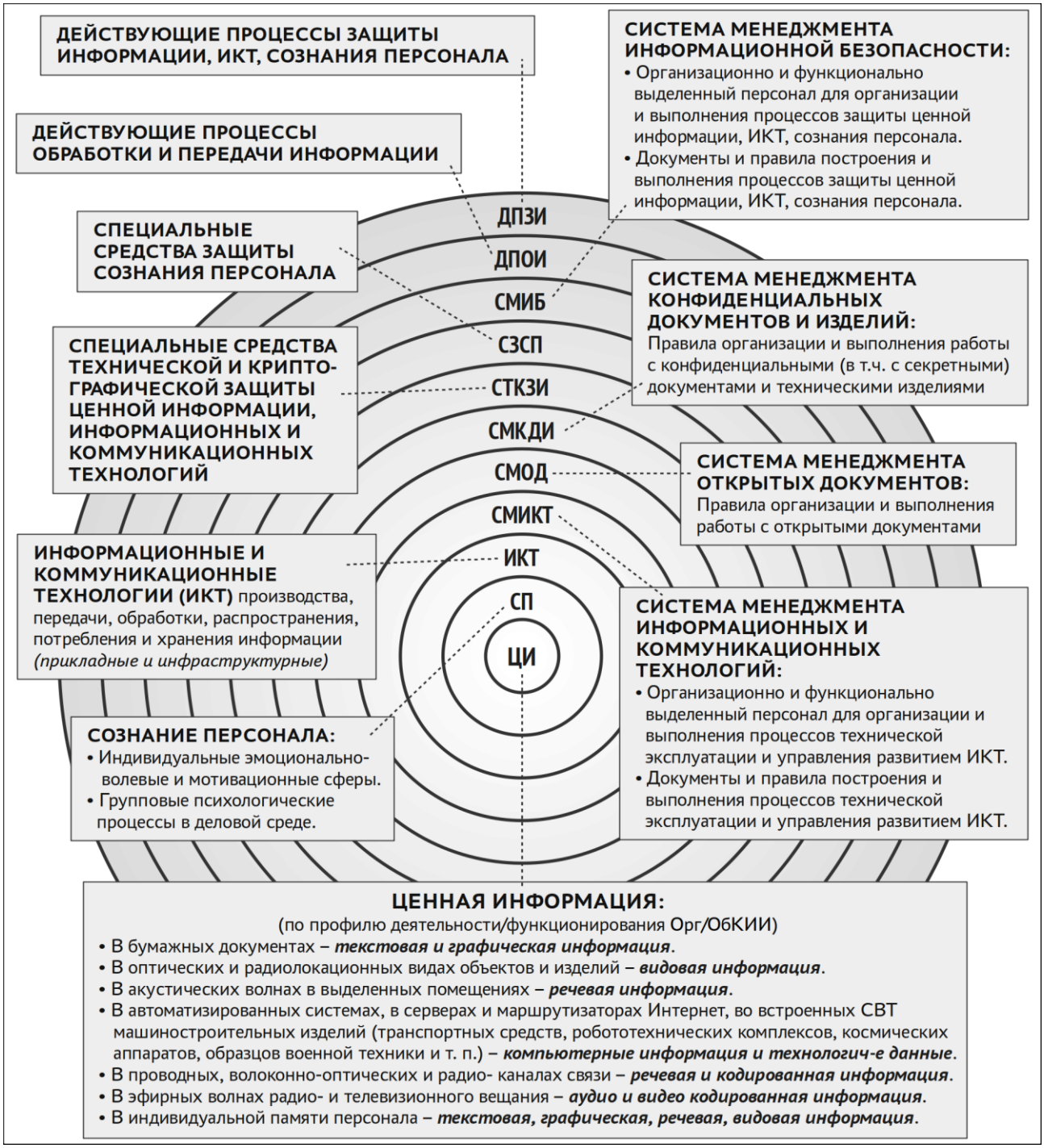

Рис. 1. Структура информационной сферы организации / объекта критической информационной инфраструктуры

Рис. 2. Возможные угрозы безопасности для информационной сферы Орг/ОбКИИ

Типовыми угрозами безопасности инфосферы Орг/ОбКИИ являются:

1) несанкционированные прочтение, просмотр, копирование, изменение, разглашение конфиденциальных информации, передача конфиденциальной информации или конфиденциальных изделий посторонним лицам. Утеря конфиденциальных документов или машинных носителей с конфиденциальной информацией, утеря конфиденциальных изделий;
2) утечка конфиденциальной информации по каналам технических разведок;
3) фальсификация ценной информации в АС и в КС;

4) физическое повреждение, уничтожение, кража вычислительной техники, связного оборудования, документов и машинных носителей с ценной информацией, конфиденциальных технических изделий;
5) радиоэлектронное подавление (РЭП) СВТ и КС, влекущее нарушение процессов их функционирования;
6) ИТВ на АС, на компьютеризированные машиностроительные изделия (КМСИ – транспортные средства, робототехнические комплексы, космические аппараты, образцы военной техники и т. п.), принадлежащие Орг/ОбКИИ;
7) ИПВ на персонал;
8) непреднамеренные ошибки и умышленное вредительство системных администраторов АС и администраторов ИБ.

Понимание автором термина «информационно-техническое воздействие» изложено в статье [21].

Ценной информацией в Орг/ОбКИИ может быть:
- в бумажных документах – текстовая и графическая информация;
- в оптических и радиолокационных видах объектов и изделий – видовая информация;
- в акустических волнах в выделенных помещениях – речевая информация;
- в АС, в серверах и маршрутизаторах Интернет, во встроенных СВТ машиностроительных изделий – компьютерные информация и компьютерные технологические данные;
- в проводных, волоконно-оптических и радио- каналах связи – речевая и кодированная информация;
- в эфирных волнах радио- и телевизионного вещания – аудио и видео кодированная информация;
- в индивидуальной памяти персонала – текстовая, графическая, речевая, видовая информация.

Виды защитных мероприятий, соответствующих этим типам угроз, приведены в таблице 1.

Таблица 1 – Соотношение видов защищаемой информации в Орг/ОбКИИ, типов возможных угроз её безопасности и видов защитных мероприятий

Виды защищаемой ценной информации	**Типы возможных угроз безопасности информации**	**Тип ущерба ценной информации**	**Виды мероприятий по защите информации***
Информация на бумажных носителях и на съёмных машинных носителях	Несанкционированные и умышленные: повреждение, уничтожение, утеря, копирование, передача посторонним лицам	Нарушение конфиденциальности, целостности, доступности	Выполнение нормативных требований режимов конфиденциальности (секретности) и правил открытого документооборота
Видовая информация	Утечка по каналам технических разведок	Нарушение конфиденциальности	Противодействие техническим разведкам
Речевая информация в выделенных помещениях	Утечка по каналам технических разведок	Нарушение конфиденциальности	Противодействие техническим разведкам

Виды защищаемой ценной информации	Типы возможных угроз безопасности информации	Тип ущерба ценной информации	Виды мероприятий по защите информации*
Речевая и кодированная информация в аналоговых телефонных системах и каналах связи	Утечка по каналам технических разведок	Нарушение конфиденциальности	Противодействие техническим разведкам, кодирование (скремблирование, шифрование)
	Фальсификация	Нарушение достоверности	Обеспечение имитостойкой связи
	Радиоэлектронное подавление	Нарушение целостности, доступности	Комплексный технический контроль (КТК) радиоизлучений, радиоэлектронная защита, ликвидация источников преднамеренных радиопомех и силового электромагнитного излучения (ЭМИ)
	Физическое повреждение, разрушение, уничтожение коммуникационного оборудования, кабельных каналов связи и систем их электропитания	Нарушение доступности	Физическая защита коммуникационного оборудования, кабельных каналов связи и систем их электропитания
Кодированная информация в цифровых радио-, волоконно-оптических и проводных системах и каналах связи и передачи данных	Утечка по каналам технических разведок	Нарушение конфиденциальности	Противодействие техническим разведкам, шифрование
	Фальсификация	Нарушение достоверности	Обеспечение имитостойкой связи
	Радиоэлектронное подавление	Нарушение целостности, доступности	КТК радиоизлучений, радиоэлектронная защита, ликвидация источников преднамеренных радиопомех и силового ЭМИ
	Информационно-техническое воздействие (компьютерные атаки)	Нарушение целостности, доступности	Техническая (аппаратно-программная и программная) защита от компьютерных атак
	Физическое повреждение, разрушение, уничтожение коммуникационного оборудования, кабельных каналов связи систем их электропитания	Нарушение доступности	Физическая защита коммуникационного оборудования, кабельных каналов связи и систем их электропитания

Виды защищаемой ценной информации	Типы возможных угроз безопасности информации	Тип ущерба ценной информации	Виды мероприятий по защите информации*
Компьютерные информация, данные, программы: - в автоматизированных системах (в т. ч. в автономных АРМах); - в персональных компьютерах, в планшетах и смартфонах для удалённой работы; - в технических изделиях (в транспортных средствах, в робототехнических комплексах, в космических аппаратах, в образцах военной техники и т. п.)	Утечка по каналам технических разведок (через ПЭМИН вычислительной техники и с использованием средств технических компьютерных разведок)	Нарушение конфиденциальности	КТК радиоизлучений, противодействие техническим разведкам
	Несанкционированный доступ (НСД)	Нарушение конфиденциальности	Защита от НСД
	Несанкционированное воздействие (НСВ)	Нарушение целостности, доступности	Защита от НСД/НСВ
	Фальсификация	Нарушение достоверности	Применение электронной подписи
	Радиоэлектронное подавление	Нарушение целостности, доступности	КТК радиоизлучений, радиоэлектронная защита, ликвидация источников преднамеренных радиопомех и силового ЭМИ
	Физическое повреждение, разрушение, уничтожение средств вычислительной техники (СВТ) и систем электропитания СВТ	Нарушение целостности, доступности	Физическая защита СВТ и систем их электропитания
Компьютерные информация, данные, программы в серверах и в маршрутизаторах Интернет	Несанкционированный доступ	Нарушение конфиденциальности	Защита от НСД
	Несанкционированное воздействие	Нарушение целостности, доступности	Защита от НСД/НСВ
	Радиоэлектронное подавление	Нарушение целостности, доступности	КТК радиоизлучений, радиоэлектронная защита, ликвидация источников преднамеренных радиопомех и силового ЭМИ
	Физическое повреждение, разрушение, уничтожение средств вычислительной техники (СВТ)	Нарушение целостности, доступности	Физическая защита СВТ
Общественная информация в сигналах радио- и телевизионного вещания	Физическое повреждение, разрушение, уничтожение технических средств передающих радио- и телецентров	Нарушение доступности	Физическая защита технических средств передающих радио- и телецентров
	Радиоэлектронное подавление	Нарушение целостности, доступности	КТК радиоизлучений, радиоэлектронная защита, ликвидация источников преднамеренных радиопомех и силового ЭМИ
Видовая, речевая, текстовая, графическая информация в индивидуальной памяти персонала	Разглашение, передача конфиденциальной информации (КИ) посторонним лицам. Запись КИ в электронную память персональных компьютеров, планшетов и смартфонов, её последующая утечка и передача посторонним лицам.	Нарушение конфиденциальности	Обучение персонала, противодействие информационно-психическим и другим вредоносным воздействиям на психику и сознание людей, противодействие агентурным разведкам

Виды защищаемой ценной информации	Типы возможных угроз безопасности информации	Тип ущерба ценной информации	Виды мероприятий по защите информации*
Все виды защищаемых активов	Непреднамеренные ошибки и умышленное вредительство системных администраторов АС и администраторов ИБ	Нарушение конфиденциальности, целостности, доступности, достоверности	(*Автор не нашёл методических и регламентирующих документов по защите от угроз этого типа*)

*) В том числе по нормативным требованиям государственных регуляторов

Информационная сфера Орг/ОбКИИ может быть разделена на следующие две части:

- *информационно-психологическая сфера* – это сознание персонала и его индивидуальные эмоционально-волевые и мотивационные сферы, групповые психологические процессы в корпоративной среде, специальные средства и процессы защиты сознания персонала от ИПВ;
- *информационно-техническая сфера* – это все остальные компоненты информационной сферы Орг/ОбКИИ, связанные с техникой и информационными технологиями.

Индивидуальная эмоционально-волевая сфера человека – это комплекс из его психологических переживаний, ощущений приятного или неприятного отношения к миру и людям с его способностями сознательно управлять своей психикой и поступками [23].

Индивидуальная мотивационная сфера человека – это комплекс его личностных ценностей, интересов, мотивов, потребностей, целей, задач, желаний и намерений [23].

Групповые психологические процессы – это процессы формирования, функционирования, совместимости, сотрудничества групп работников в деловой корпоративной среде, а также процессы развития конфликтности [23].

Термины «информационно-психологическая сфера», «информационно-психологическая безопасность», «информационно-техническая сфера», «информационно-техническая безопасность» ранее уже рассматривались в научных публикациях, например, в работе [22].

В настоящей статье не рассматриваются содержательно информационно-психологическая сфера и вопросы её безопасности.

Определение комплекса мероприятий по обеспечению безопасности инфосферы Орг/ОбКИИ

Очевидно, что деятельность по обеспечению безопасности инфосферы Орг/ОбКИИ должна быть организованной и управляемой. Существующие нормативные требования и рекомендации по системной организации и управлению информационной безопасностью содержаться:

- в государственных ведомственных положениях и инструкциях по организации и функционированию режима секретности;
- в государственных ведомственных и в корпоративных положениях и инструкциях по организации и функционированию режимов служебной и коммерческой тайн;

- в нормативных требованиях государственных регуляторов по противодействию техническим разведкам, по технической защите информации, по защите государственных систем связи, по комплексному техническому контролю радиоизлучений;
- в других документах корпоративного управления негосударственных организаций;
- в российских [2-7] и международных [8-13] стандартах по менеджменту информационной безопасности.

В предметных рамках настоящей статьи интерес представляет возможная логическая схема применения рекомендаций стандартов серии 270xx [2-13] к управлению безопасностью инфосферы Орг/ОбКИИ. Стандарты этой серии в настоящее время активно развиваются и обновляются (так, например, в 2013 году обновились вторыми редакциями стандарты ISO/IEC 27001 и 27002 [9, 10], в 2018 году обновился пятой редакцией корневой стандарт ISO/IEC 27000 [8]).

Более ранний ГОСТ 13335-1–2006 [24] концептуально и содержательно не расходится со стандартами серии 270xx, но описывает менеджмент ИБ кратко как деятельность вообще и без определения СМИБ.

Стандарт ISO/IEC 27001:2013(E) [9] определяет следующие семь функциональных блоков (ФБ) корпоративного менеджмента ИБ:

1-й ФБ: Определение и документирование общего контекста деятельности организации, который является существенным для построения и функционирования СМИБ (Context of the organization);

2-й ФБ: Определение и документирование лидирующей роли высшего руководства организации в достижении корпоративной ИБ, в том числе определение и персональное назначение обязанностей и полномочий по обеспечению ИБ, определение верхнеуровневой политики ИБ организации (Leadership);

3-й ФБ: Первоначальное планирование СМИБ при её внедрении, включающее определение целей СМИБ, рисков организации, связанных с ИБ, а также определение методологии работы с рисками (Planning);

4-й ФБ: Обеспечение функционирования СМИБ, включая материальные ресурсы, профессионально подготовленный и осведомлённый по ИБ персонал, выстроенные корпоративные коммуникации в СМИБ, систему документов СМИБ (Support);

5-й ФБ: Операционная деятельность – организованное исполнение всех установленных процессов и функций обеспечения ИБ, в том числе оперативное планирование и управление, оперативная оценка и обработка рисков ИБ (Operation);

6-й ФБ: Оценка результатов деятельности, включающая мониторинг, измерение, анализ и оценку процессов деятельности СМИБ, периодическое проведение внутренних аудитов деятельности СМИБ, проведение анализа деятельности СМИБ высшим руководством организации (Performance evaluation);

7-й ФБ: Необходимые улучшения СМИБ, устраняющие выявляемые недостатки и проблемы (Improvement).

Для указанного выше 3-го блока менеджмента ИБ стандарт ISO/IEC 27001:2013(E) [9] определяет набор из 114 внедряемых задач управления информационной безопасностью (control objectives) и механизмов их реализации (controls), которые сгруппированы в 14 процессных доменов. Для настоящей статьи представляет интерес процессный домен «Анализ соответствия» («Compliance»), в котором определяется поддомен «Анализ информационной безопасности» («Information security reviews»), содержащий задачу «Анализ технического соответствия» («Technical compliance review»), которые близки к логически выстраиваемому здесь комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ.

В настоящей ситуации пока нет нормативных русских перевод стандартов ISO/IEC 27001:2013(E) [9] и 27002:2013(E) [10] автором статьи предлагается следующее перечисление множества внедряемых в рамках СМИБ задач управления информационной безопасностью Орг/ОбКИИ (как безопасностью инфосферы) в авторском варианте с сокращениями, с агрегированием и с учётом российских особенностей:

1. Классификация и документированный учёт защищаемых активов: ценной информации, документов, прикладного ПО, СВТ, КС, конфиденциальных технических изделий, зданий, сооружений, помещений, в которых производится и обрабатывается ценная информация, размещаются библиотеки и архивы документов и конфиденциальные технические изделия.
2. Разработка, принятие и корректировка комплекса документированных политик ИБ.
3. Построение и изменения организационной структуры ИБ.
4. Администрирование персонала, вовлечённого в ИБ, в том числе тестирование требуемых от него специальных знаний по ИБ.
5. Физическая защита зданий, сооружений, помещений, СВТ, КС, обеспечивающих инженерных систем от несанкционированного физического проникновения, доступа, кражи, вредительства.
6. Комплексный технический контроль (КТК) радиоизлучений и радиоэлектронная защита СВТ, КС, КМСИ от РЭП.
7. Противодействие техническим разведкам.
8. Криптографическая защита информации в СВТ, КС, КМСИ.
9. Управление доступом персонала к компьютерным информации, данным и программам (в том числе разграничение прав доступа, применение программных и аппаратно-программных средств контроля доступа, контроль доступа).
10. Обеспечение эксплуатационной безопасности компьютерных информации, данных, ПО (в том числе защита от компьютерных атак и вирусов, обновление версий ПО и СВТ, резервное копирование и пр.).
11. Обеспечение безопасности сетей и информационных коммуникаций.

12. Обеспечение ИБ компьютеризированных машиностроительных изделий, а также обеспечение ИБ корпоративных мобильных телефонов и планшетов.
13. Управление доверенными закупками ПО, СВТ, средств защиты информации (СЗИ), информационных услуг.
14. Управление собственной разработкой безопасного ПО.
15. Планирование особых мероприятий ИБ для условий чрезвычайных ситуаций.
16. Мониторинг событий ИБ.
17. Управление инцидентами ИБ.
18. Управление уязвимостями ИБ.
19. Мониторинг информационно-психологических воздействий на персонал, выполнение мероприятий по защите персонала от ИПВ.
20. Контроль и обеспечение соответствия мероприятий ИБ нормативным требованиям государственных регуляторов.
21. Внутренние контроль и анализ соответствия процессов обработки и защиты информации принятым политикам и стандартам ИБ, выполняемый в Орг/ОбКИИ руководителями всех уровней.
22. Независимый внешний аудит политик, организации, процедур и технологий ИБ.
23. Анализ технического соответствия информационных систем Орг/ОбКИИ корпоративным политикам и стандартам ИБ Орг/ОбКИИ.
24. Оценка и обработка рисков деятельности/функционирования Орг/ ОбКИИ, создаваемых угрозами для ИБ Орг/ОбКИИ.

Этот комплекс мероприятий иллюстрирует рис. 3 в виде схемы, которая выполнена в нотации «Value-added Chain Diagram» (VACD – цепочка добавляемой ценности [25]).

Стандартом ISO/IEC 27002:2013(E) [10] предусмотрена возможность проведения тестирования на проникновение (penetration testing) и оценивания уязвимостей (vulnerability assessments) при выполнении задачи № 23 «Анализ технического соответствия».

Определение деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ

Исходя из данного выше перечня задач управления ИБ, осуществляемых в рамках СМИБ, автор статьи предлагает рассматривать новый вид специальной деятельности «Комплексное техническое диагностирование информационной безопасности Орг/ОбКИИ», которая заменяла бы и расширяла задачи №23 и №24, показанные на рис. 3, и которая предполагает последовательное выполнение следующих трёх задач:

1) комплексное техническое тестирование защищённости инфосферы Орг/ОбКИИ;
2) комплексный анализ и формализованное описание (моделирование) возможных угроз безопасности инфосферы Орг/ОбКИИ;

3) комплексное оценивание рисков деятельности / функционирования Орг/ОбКИИ и разработка предложений по их обработке.

При этом деятельность «Комплексное техническое диагностирование информационной безопасности Орг/ОбКИИ» может:

- во-первых, быть лицензируемой и оказываться как услуга;
- во-вторых, выполняться собственными подразделениями ИБ и ИКТ в Орг/ОбКИИ, либо выполняться внешней подрядной организацией.

Соответствующий новый вариант состава задач управления информационной безопасностью Орг/ОбКИИ (как безопасностью инфосферы) показан на рис. 4, а иерархическая структура задач деятельности «Комплексное техническое диагностирование информационной безопасности Орг/ОбКИИ» показана на рис. 5 в нотации «VACD».

На рис. 6 показаны в нотации «Idef0» три верхнеуровневые задачи комплексного технического диагностирования информационной безопасности Орг/ОбКИИ вместе со связывающими их информационными потоками [25].

В расширение множества идей, предложенных в монографии [19], можно предложить следующее классификационное разделение указанной выше первой задачи – комплексного технического тестирования защищённости инфосферы Орг/ОбКИИ – на следующие три подзадачи:

1) безопасное техническое тестирование реально функционирующих систем и средств информатизации и связи Орг/ОбКИИ без рисков нарушения выполняемых управленческих и технологических процессов в Орг/ОбКИИ;
2) построение моделирующего диагностического стенда (стендового полигона) информационной безопасности Орг/ОбКИИ, на котором возможно натурное моделирование ИТ-архитектуры Орг/ОбКИИ и опасных инцидентов информационной безопасности Орг/ОбКИИ с имитацией значительных нарушений и блокировок моделируемых управленческих и технологических процессов Орг/ОбКИИ;
3) техническое тестирование защищённости натурной стендовой модели инфосферы Орг/ОбКИИ модельными подавляющими радиопомехами и модельными поражающими ИТВ с модельным воспроизведением опасных инцидентов информационной безопасности Орг/ОбКИИ.

Выполнение первой из этих трёх подзадач может включать:

- безопасное техническое тестирование физической защищённости зданий, сооружений, помещений, СВТ, КС, КМСИ, а также обеспечивающих их инженерных средств от несанкционированного физического доступа, от повреждения, от кражи;
- безопасное техническое тестирование (выявление) технических каналов утечки информации по акустическим, по радио, по визуальным каналам из выделенных помещений, из СВТ, из КС, из КМСИ;
- безопасное техническое тестирование программно-алгоритмической защищённости СВТ, КС, КМСИ с применением средств и методов технической компьютерной разведки – безопасное «тестирование на проникновение».

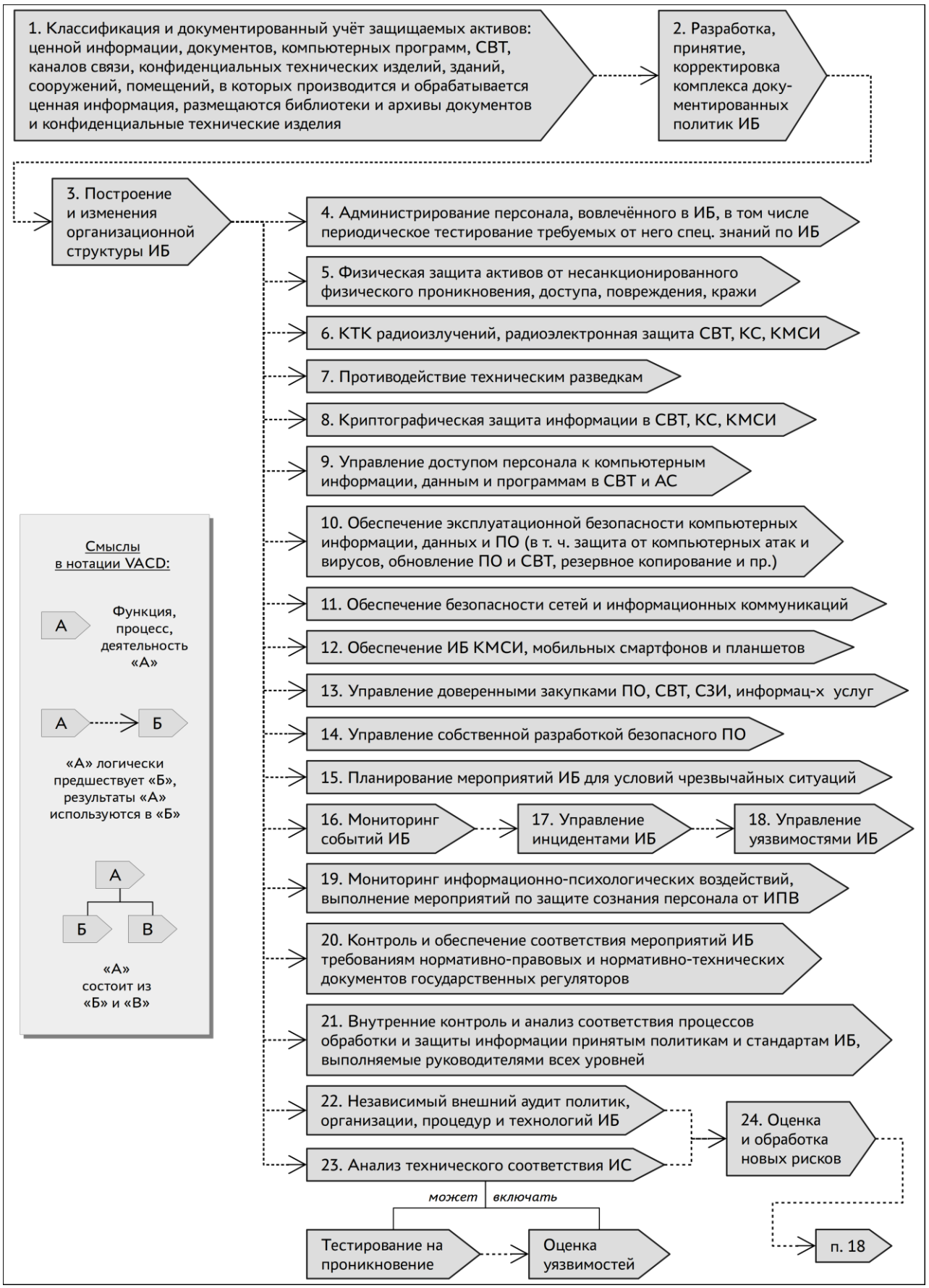

Рис. 3. Стандартный состав и связи комплекса мероприятий обеспечения безопасности инфосферы Орг/ОбКИИ, осуществляемых в рамках СМИБ

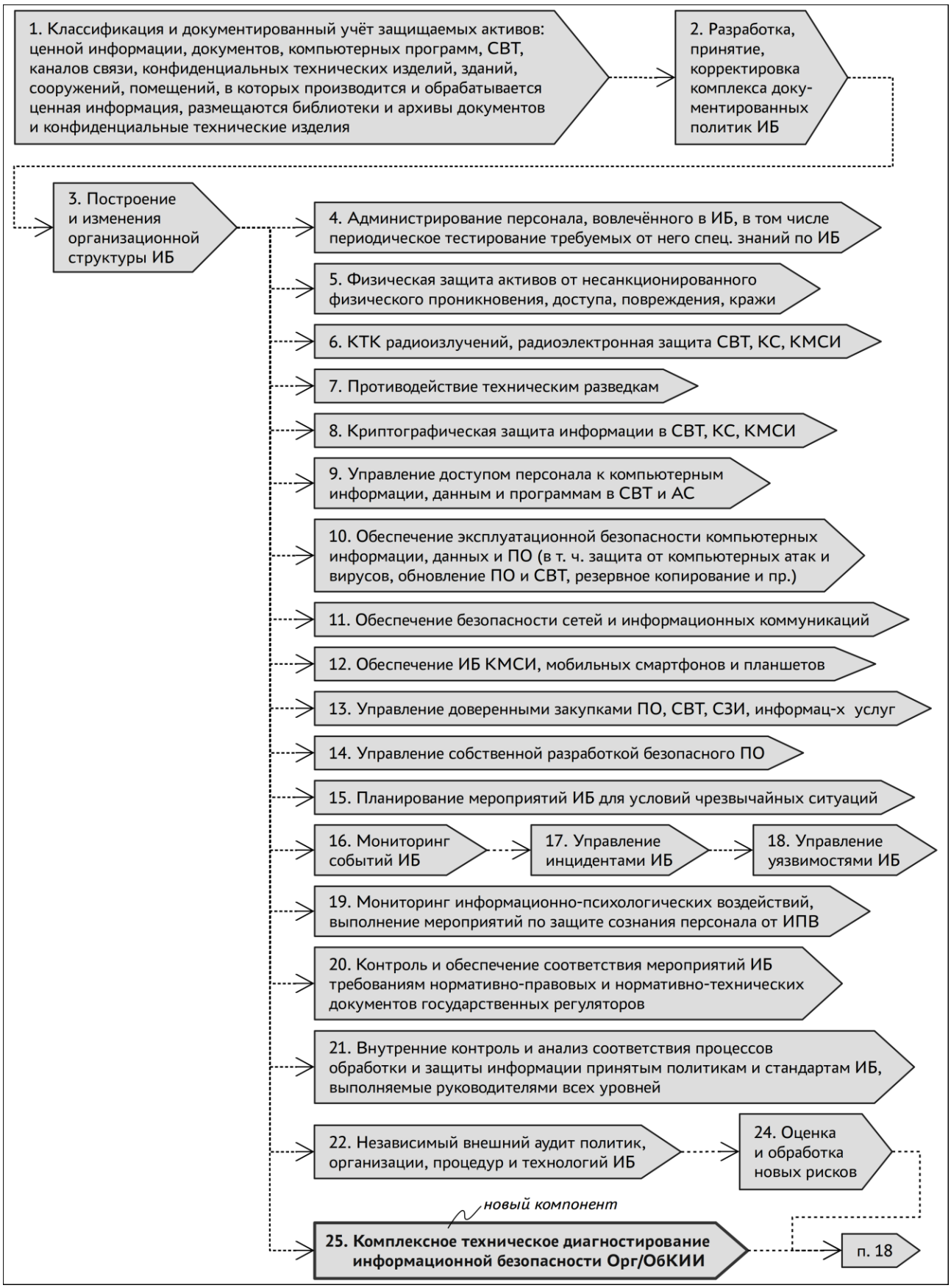

Рис. 4. Новый вариант состава и связей комплекса мероприятий обеспечения безопасности инфосферы Орг/ОбКИИ, осуществляемых в рамках СМИБ

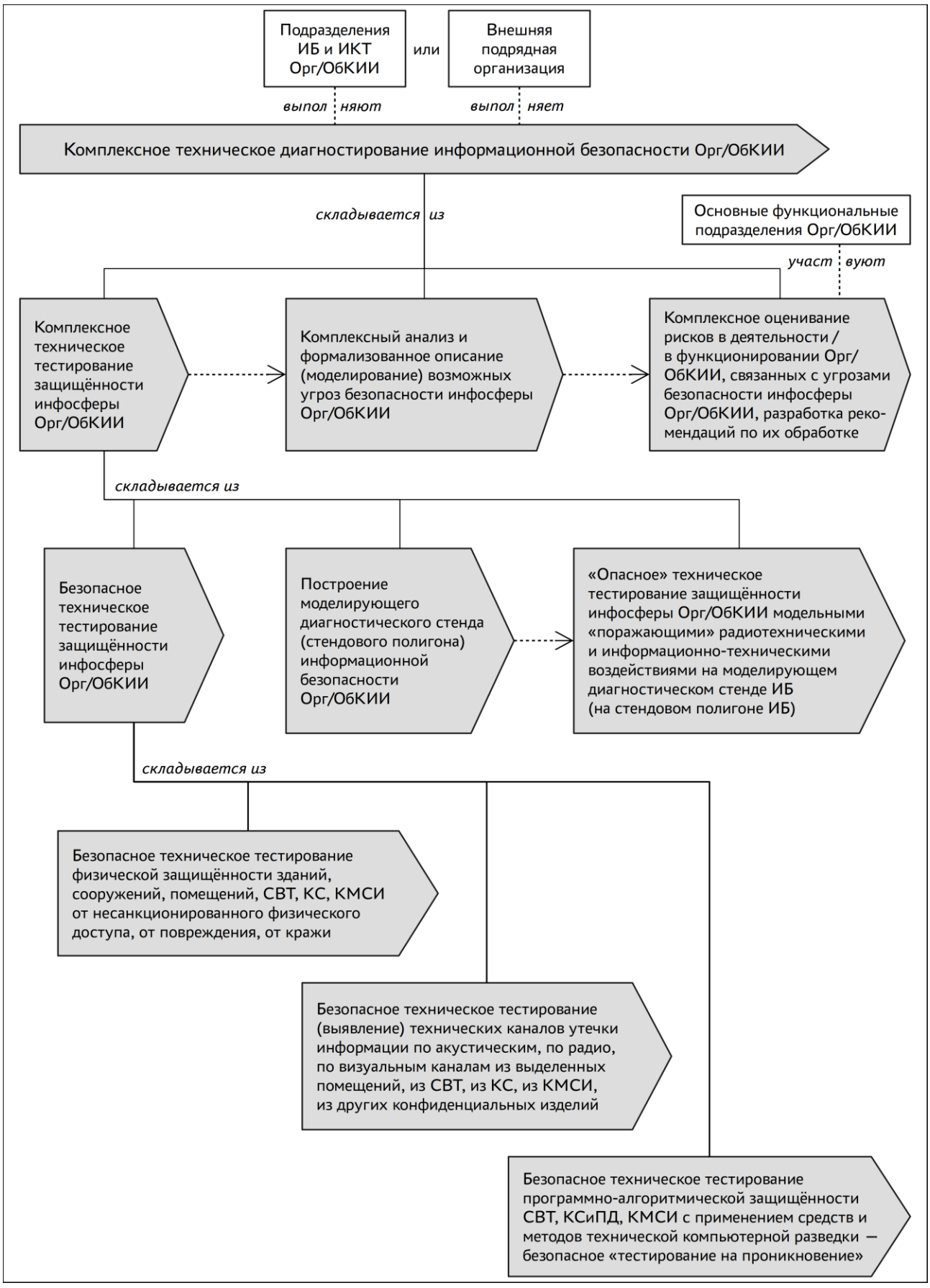

Рис. 5. Состав и логические связи задач комплексного технического диагностирования информационной безопасности Орг/ОбКИИ

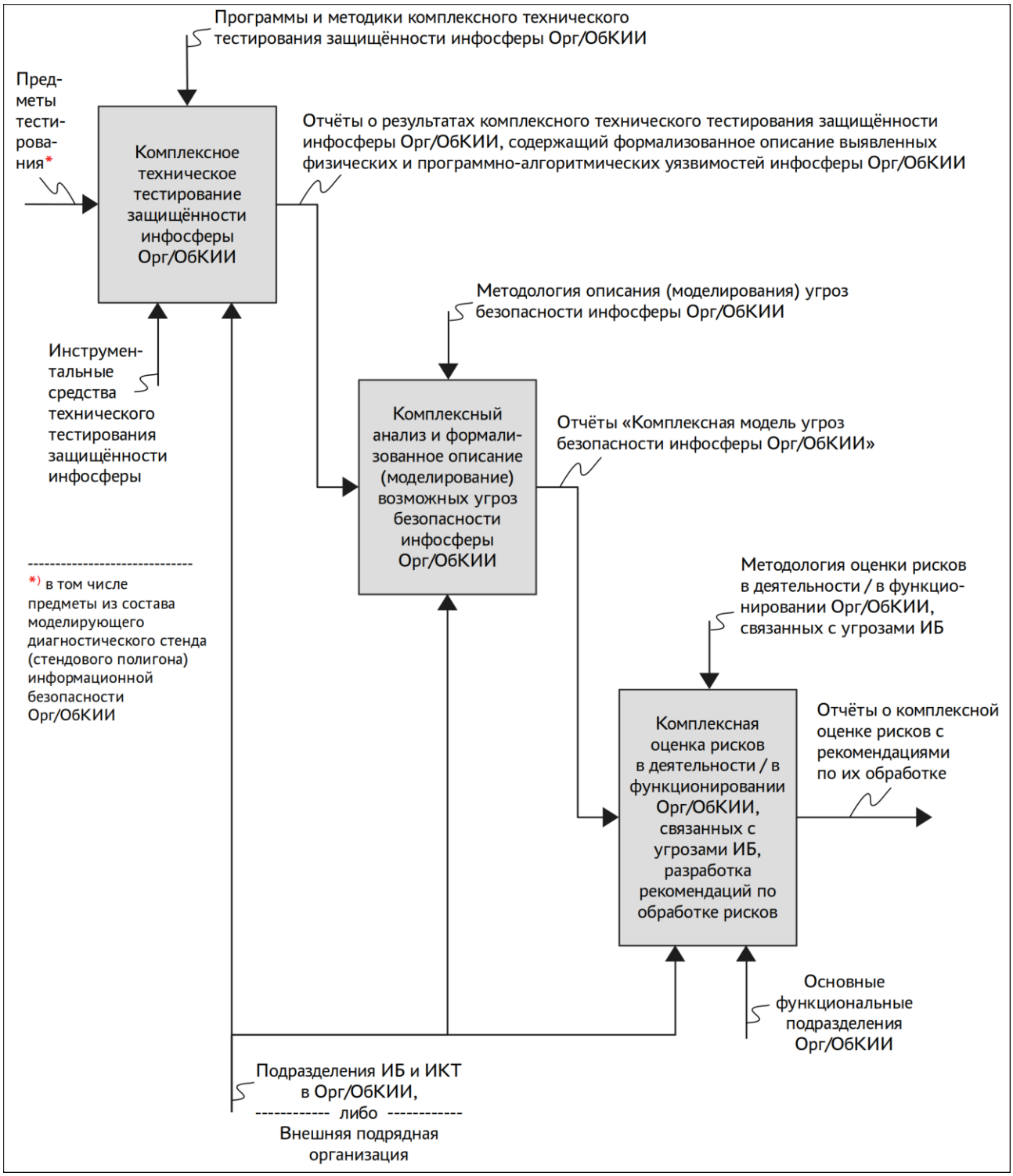

Рис. 6. Информационные потоки в деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ

На рис. 7 изображена семантическая сеть (схема) процессной функции комплексного технического тестирования защищённости инфосферы Орг/ОбКИИ (нотация семантических сетей поясняется, например, в работе [26]).

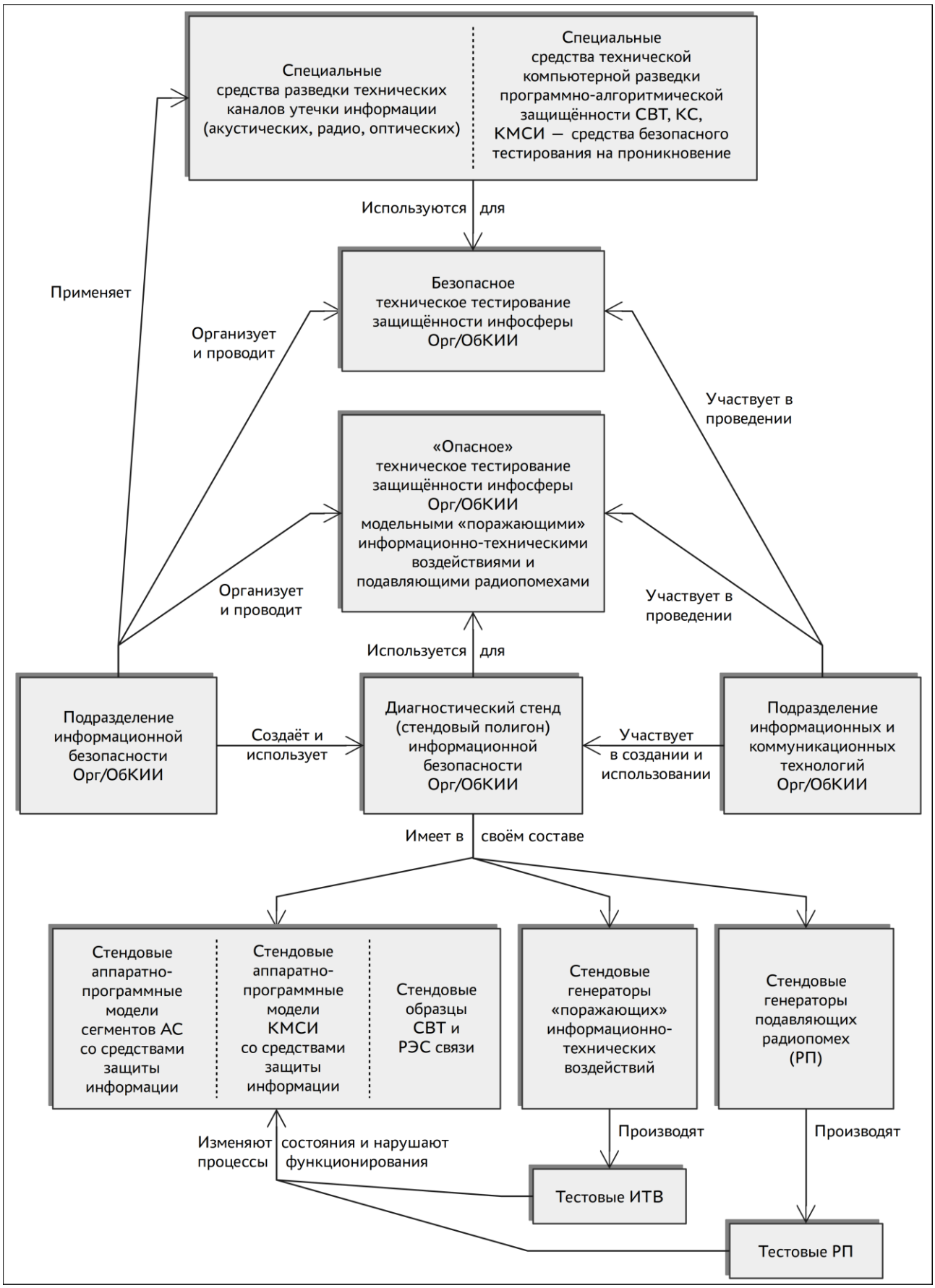

Рис. 7. Семантическая схема процессной функции комплексного технического тестирования защищённости инфосферы Орг/ОбКИИ

Обобщая выполненный логический анализ возможной деятельности по комплексному техническому диагностированию защищённости инфосферы Орг/ОбКИИ и ориентируясь на терминологические рекомендации ГОСТ 20911-89 [27], можно дать следующее определение.

Комплексное техническое диагностирование информационной безопасности организации / значимого объекта критической информационной инфраструктуры – организованная профессиональная деятельность по определению состояния защищённости технической информационной сферы организации/объекта критической информационной инфраструктуры, выполняемая с применением специальных знаний, нормативов и технологий.

Определение новых научно-технических задач, связанных с постановкой комплексного технического диагностирования информационной безопасности Орг/ОбКИИ

Предлагаемая новая деятельность по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ может использовать следующие известные методы и средства:

- методы и технические средства комплексных специальных проверок для выявления технических каналов утечек информации (рассматриваются, например, в работе [28]);
- методы и технические средства комплексного технического контроля радиоизлучений (рассматриваются, например, в работе [29]);
- методы и программные средства российских разработчиков для тестирования защищённости ИС, например, «Max Patrol» [30] и «RedCheck» [31] (сравнительный анализ некоторых российских и зарубежных методов и средств тестирования ИС есть в статье [32]);
- зарубежные методы тестирования на проникновение: «The Open Source Security Testing Methodology Manual» (OSSTMM) [33], «Penetration Testing Execution Standard» (PTES) [34], «Technical Guide to Information Security Testing and Assessment» [35], «Information System Security Assessment Framework» (ISSAF) [36], «A Penetration Testing Model» [37];
- разработанные ФСТЭК России методика [38] оценки и базовая модель угроз [39] безопасности персональных данных (примером иного моделирования угроз является модель, описанная в статье [40]);
- методы оценки рисков ИБ, изложенные в стандартах [7, 13, 41].

Этот перечень может быть дополнен новыми методами, которых пока нет, но разработка которых может стать решением множества новых научно-технических задач, связанных с постановкой и развитием деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ, в том числе разработка:

- набора стандартов деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ;
- нормативных требований к организации и порядку проведения комплексного технического диагностирования информационной безопасности Орг/ОбКИИ различных классов и категорий, в том числе с учётом

условий обработки в Орг/ОбКИИ информации, составляющей государственную, коммерческую и служебную тайны;
- методов построения моделирующих диагностических стендов (стендовых полигонов) информационной безопасности Орг/ОбКИИ;
- методов построения и применения генераторов тестовых поражающих информационно-технических воздействий, а также нормативных требований к этим генераторам;
- методов количественного оценивания защищённости инфосферы Орг/ОбКИИ, проводимого по результатам комплексного технического диагностирования информационной безопасности Орг/ОбКИИ.

Видится также возможным включение деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ в перечень лицензируемых услуг, предусмотренных общим лицензированием деятельности по технической защите конфиденциальной информации [42].

И в завершение статьи, подобно тому как в стандарте [27] определён термин *«техническая диагностика»*, можно определить следующий термин:

Комплексная техническая диагностика информационной безопасности – область знаний и практической деятельности, охватывающая теорию, технологии и практику оценивания состояния защищённости технической информационной сферы организаций и значимых объектов КИИ.

Такое терминологическое определение открывает широкую перспективу для активации и научно-технического развития деятельности по комплексному техническому диагностированию ИБ организаций и значимых объектов КИИ.

Заключение

В результате выполненного логического проецирования положений Доктрины ИБ о безопасности информационной сферы страны на уровень организаций и значимых объектов критической информационной инфраструктуры в статье решена актуальная теоретическая задача разработки логической модели возможной деятельности по комплексному техническому диагностированию защищённости (безопасности) инфосферы Орг/ОбКИИ.

В статье, в рамках решения этой теоретической задачи, предложены:
- определение понятия информационной сферы Орг/ОбКИИ;
- систематизированное описание возможных типовых угроз безопасности инфосферы Орг/ОбКИИ и видов защитных мероприятий;
- логическая модель комплексного технического диагностирования безопасности инфосферы Орг/ОбКИИ;
- логическая модель процессной функции комплексного технического тестирования защищённости инфосферы Орг/ОбКИИ с использованием моделирующего диагностического стенда (стендового полигона) информационной безопасности Орг/ОбКИИ;
- перечень новых научно-технических задач, которые могут решаться в интересах практической реализации логической модели комплексной технической диагностики информационной безопасности Орг/ОбКИИ;

- определения новых терминов «комплексное техническое диагностирование информационной безопасности» и «комплексная техническая диагностика информационной безопасности» организаций и значимых объектов критической информационной инфраструктуры.

Выражено также авторское предположение о потенциальной возможности государственного лицензирования деятельности по комплексному техническому диагностированию информационной безопасности Орг/ОбКИИ как услуги, которая может быть подготовлена к реализации после проведения множества необходимых теоретических и технологических разработок.

Приложение

Авторские определения некоторых терминов, используемых в статье

Конфиденциальная информация – информация, к которой ограничен персональный доступ. Конфиденциальная информация должна производиться и использоваться в специальных условиях и по специальным правилам, которые установлены в организации нормативными правовыми и/или корпоративными документами.

Конфиденциальность информации – абстрактный признак информации, обозначающий её принадлежность к категории конфиденциальной и обязывающий лиц к ней допущенных выполнять установленные правила её производства и использования. Для обозначения конфиденциальной информации на её носителях могут записываться специальные атрибутивные метки (например, гриф секретности).

Уровень (степень) конфиденциальности информации – определённый в нормативных и/или регламентирующих документах государства/организации профиль ограничения персонального доступа к конфиденциальной информации.

Определение уровней (степеней) конфиденциальности информации обычно связывается с определением соответствующих уровней (степеней) ущерба безопасности государства/организации, наносимого вследствие несанкционированной утечки конфиденциальной информации, и выражается (представляется) в виде упорядоченного набора (шкалы) значений, отражающих различные объёмы ограничений персонального доступа к конфиденциальной информации. Примером является набор степеней секретности, которые определены в Законе РФ от 21.07.1993 № 5485-1 «О государственной тайне».

Нарушение конфиденциальности информации – процесс и произошедшее событие персонального доступа к конфиденциальной информации, совершённого с нарушением установленных условий и правил доступа к конфиденциальной информации.

Целостная информация – информация, которая не изменялась при хранении или использовании, либо изменялась по установленным правилам.

Целостность информации – абстрактный признак информации, обозначающий её целостное состояние. Целостность информации может проверяться специальными доказательными процедурами.

Нарушение целостности информации – процесс и произошедшее событие изменения информации, совершённого с нарушением установленных правил.

Доступная информация – информация, которая может быть запрошена и получена лицами (пользователями) или автоматически выполняемыми технологическими процессами обработки информации, имеющими разрешение на доступ к ней, в установленном порядке в течение интервала времени, продолжительность которого определена как нормативная или является субъективно приемлемой для пользователей.

Доступность информации – абстрактный признак информации, обозначающий наличие комплекса действующих условий и правил, в рамках которых информация является доступной для пользователей или для автоматически выполняемых технологических процессов обработки информации.

Нарушение доступности информации – процесс и произошедшее событие изменения комплекса условий и правил предоставления информации, приведшее к блокированию возможности отправления запросов на получение информации или приведшее к неприемлемому увеличению продолжительности ожидания получения информации по выданным запросам.

Достоверная информация – информация, которая поступает из доверенного источника и точно отражает/передаёт факты, документы, управленческие распоряжения (команды, приказы).

Недостоверная (фальсифицированная) информация – информация, которая поступает из недостоверного источника и/или передаёт намеренно ложные факты, документы, управленческие распоряжения (команды, приказы).

Достоверность информации – абстрактный признак информации, обозначающий её принадлежность к категории достоверной. Достоверность информации может проверяться специальными доказательными процедурами.

Нарушение достоверности (фальсификация) информации – процесс и произошедшее событие производства и передачи недостоверной (фальсифицированной) информации.

Защищённая информация – информация, для которой созданы и действуют специальные условия и правила, в которых и по которым информация является конфиденциальной и/или целостной и/или доступной, и/или достоверной и которые препятствуют полной или частичной реализации угроз её безопасности в соответствии с принятыми рисками информационной безопасности.

Защищённость информации – абстрактный признак информации, обозначающий её принадлежность к категории защищённой.

Литература

1. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации [Электронный ресурс]. 06.12.2016. –

URL:
http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (дата обращения: 12.09.2019).

2. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.12.2013. – URL: http://protect.gost.ru/document.aspx?control=7&id=183445 (дата обращения: 12.09.2019).

3. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.02.2008. – URL: http://protect.gost.ru/document.aspx?control=7&id=129018 (дата обращения: 12.09.2019).

4. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Свод норм и правил менеджмента информационной безопасности // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.01.2014. – URL: http://protect.gost.ru/document.aspx?control=7&id=183918 (дата обращения: 12.09.2019).

5. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.12.2013. – URL: http://protect.gost.ru/document.aspx?control=7&id=183599 (дата обращения: 12.09.2019).

6. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Измерения // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.01.2012. – URL: http://protect.gost.ru/document.aspx?control=7&id=179060 (дата обращения: 12.09.2019).

7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.12.2011. – URL: http://protect.gost.ru/document.aspx?control=7&id=177398 (дата обращения: 12.09.2019).

8. ISO/IEC 27000:2018(E). Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary // Интернет-портал организации «International Organization for Standardization» [Электронный ресурс]. 01.02.2018. – URL: https://www.iso.org/ru/standard/73906.html (дата обращения: 12.09.2019).

9. ISO/IEC 27001:2013(E). Information Technology – Security Techniques – Information Security Management Systems – Requirements // Интернет-портал организации «International Organization for Standardization» [Электронный ресурс]. 01.10.2013. – URL: https://www.iso.org/ru/standard/54534.html (дата обращения: 12.09.2019).

10. ISO/IEC 27002:2013(E). Information Technology – Security Techniques – Code of Practice for Information Security Controls // Интернет-портал организации «International Organization for Standardization» [Электронный ресурс]. 01.10.2013. – URL: https://www.iso.org/ru/standard/54533.html (дата обращения: 12.09.2019).

11. ISO/IEC 27003:2017(E). Information Technology – Security Techniques – Information Security Management System Implementation Guidance // Интернет-портал организации «International Organization for Standardization» [Электронный ресурс]. 01.03.2017. – URL: https://www.iso.org/standard/63417.html (дата обращения: 12.09.2019).

12. ISO/IEC 27004:2016(E). Information technology – Security techniques – Information security management – Measurement // Интернет-портал организации «International Organization for Standardization» [Электронный ресурс]. 01.12.2016. – URL: https://www.iso.org/standard/64120.html (дата обращения: 12.09.2019).

13. ISO/IEC 27005:2018(E). Information Technology – Security Techniques – Information Security Risk Management // Интернет-портал организации «International Organization for Standardization» [Электронный ресурс]. 01.07.2018. – URL: https://www.iso.org/ru/standard/75281.html (дата обращения: 12.09.2019).

14. Климов С. М., Сычёв М. П. Стендовый полигон учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. № 24. С. 206-213.

15. Климов С. М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27-36.

16. Климов С. М., Зорин Э. Ф., Половников А. Ю., Антонов С. Г. Основные направления обеспечения информационной безопасности ракетных комплексов стратегического назначения в условиях информационно-технических воздействий // Военная мысль. 2016. № 6. С. 24–29.

17. Шевырев А. В., Невзоров Ю. В., Пименов П. Н., Фомина И. А., Пронин С. А. Анализ устойчивого функционирования робототехнических комплексов нового поколения в условиях преднамеренного воздействия сверхкоротких электромагнитных импульсов // Известия ЮФУ. Технические науки. 2016. № 2 (175). С. 240-251.

18. Тихонов Р. И., Бубенщиков Ю. Н. Практический опыт испытаний комплексов с беспилотными летательными аппаратами в условиях информационно-технических воздействий // Военная мысль. 2019. № 6. С. 118–124.

19. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с. – URL: http://sccs.intelgr.com/editors/Makarenko/makarenko-audit_ib_2018.pdf (дата обращения: 12.09.2019).

20. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены приказом директора ФСТЭК России от 25 декабря 2017 года № 239 // Интернет-портал ФСТЭК России [Электронный ресурс]. 25.12.2017. – URL: https://fstec.ru/component/attachments/download/1879 (дата обращения: 12.09.2019).

21. Забегалин Е. В. К вопросу об определении термина «информационно-техническое воздействие» // Системы управления, связи и безопасности. 2018. № 2. С. 121-150. – URL: http://sccs.intelgr.com/archive/2018-02/08-Zabegalin.pdf (дата обращения: 12.09.2019).

22. Баришполец В. А. Информационно-психологическая безопасность: основные положения // Радиоэлектроника. Наносистемы. Информационные технологии. 2013. Т. 5, № 2. С. 62-104.

23. Морозов А. В. Деловая психология. Курс лекций; Учебник для высших и средних специальных учебных заведений. – СПб.: Издательство Союз, 2000. – 576 с.

24. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.06.2007. – URL: http://protect.gost.ru/document1.aspx?control=31&id=128738 (дата обращения: 12.09.2019).

25. Репин В. В., Елиферов В. Г. Процессный подход к управлению. Моделирование бизнес-процессов. – М.: Манн, Иванов и Фербер, 2013. – 544 с.

26. Горчаков Л. В., Стась А. Н. Основы искусственного интеллекта: учебное пособие. – Томск: Изд-во ТГПУ, 2006. – 199 с. – URL: http://koi.tspu.ru/koi_books/gorchakov5/Index.html (дата обращения: 12.09.2019).

27. ГОСТ 20911–89. Техническая диагностика. Термины и определения // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.06.2007. – URL: http://protect.gost.ru/document.aspx?control=7&id=138613 (дата обращения: 12.09.2019).

28. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2017. – 586 с.

29. Игнатенков В. Г., Сахнин А. А. Защищенное информационное пространство. Комплексный технический контроль радиоэлектронных средств. – М.: Горячая линия – Телеком, 2016. – 336 с.

30. Система контроля защищённости и соответствия стандартам «Max Patrol» // Интернет-портал компании «Positive Technologies» [Электронный ресурс]. 2018. – URL:

https://www.ptsecurity.com/upload/corporate/ru-ru/products/mp8/PT-MaxPatrol-Data-Sheet-rus.pdf (дата обращения: 12.09.2019).

31. Комплексное решение для аудита безопасности IT-инфраструктуры предприятия (сканер безопасности) «RedCheck» // Интернет-сайт продукта «RedCheck» компании «АЛТЭКС-СОФТ» [Электронный ресурс]. 2015. – URL: https://www.redcheck.ru/lib/f/buklet.pdf (дата обращения: 12.09.2019).

32. Богораз А. Г., Пескова О. Ю. Методика тестирования и оценки межсетевых экранов // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 148-156.

33. The Open Source Security Testing Methodology Manual (OSSTMM) // Интернет-портал организации «The Institute for Security and Open Methodologies» (ISECOM) [Электронный ресурс]. 15.12.2010. – URL: http://www.isecom.org/mirror/OSSTMM.3.pdf (дата обращения: 12.09.2019).

34. The Penetration Testing Execution Standard (PTES) // Интернет-сайт стандарта «PTES» [Электронный ресурс]. 30.04.2012. – URL: http://www.pentest-standard.org (дата обращения: 12.09.2019).

35. Murugiah P. Souppaya, Karen A. Scarfone. Technical Guide to Information Security Testing and Assessment. NIST Special Publications 800-115 // Интернет-портал организации «The National Institute of Standards and Technology» (NIST) [Электронный ресурс]. 30.09.2008. – URL: https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment (дата обращения: 12.09.2019).

36. The Information System Security Assessment Framework (ISSAF) // Интернет-портал «SourceForge» [Электронный ресурс]. 2014. – URL: https://sourceforge.net/projects/isstf/ (дата обращения: 12.09.2019).

37. A Penetration Testing Model // Интернет-портал организации «Bundesamt für Sicherheit in der Informationstechnik» (BSI) [Электронный ресурс]. 21.12.2004. – – URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html (дата обращения: 12.09.2019).

38. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г. // Интернет-портал ФСТЭК России [Электронный ресурс]. 09.01.2008. – URL: https://fstec.ru/component/attachments/download/290 (дата обращения: 12.09.2019).

39. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. // Интернет-портал ФСТЭК России [Электронный ресурс]. 09.01.2008. – URL: https://fstec.ru/component/attachments/download/289 (дата обращения: 12.09.2019).

40. Андреев А. Г., Казаков Г. В., Корянов В. В. Модель угроз информационной безопасности автоматизированной системы подготовки

данных управления летательными аппаратами и модель защиты // Известия высших учебных заведений. Машиностроение. 2018. № 6 (699). С. 86-95.

41. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска // Интернет-портал ФГУП «Стандартинформ» [Электронный ресурс]. 01.12.2012. – URL: http://protect.gost.ru/document.aspx?control=7&id=179313 (дата обращения: 12.09.2019).

42. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 // Интернет-портал ФСТЭК России [Электронный ресурс]. 03.02.2012. – URL: https://fstec.ru/component/attachments/download/148 (дата обращения: 12.09.2019).

References

1. Doctrine of Information Security of the Russian Federation. *Official Internet Legal Information Portal*, 06 December 2016. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (accessed 12 September 2019) (in Russian).

2. State Standard 27000-2012. Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Sistemy Menedzhmenta Informatsionnoi Bezopasnosti. Obshchii Obzor I Terminologiia [Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary]. *FSUE «Standartinform» Internet Portal*, 01 December 2013. Available at: http://protect.gost.ru/ document.aspx?control=7&id=183445 (accessed 12 September 2019) (in Russian).

3. State Standard 27001-2006. Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Sistemy Menedzhmenta Informatsionnoi Bezopasnosti. Trebovaniia [Information Technology. Security Techniques. Information Security Management Systems. Requirements]. *FSUE «Standartinform» Internet Portal*, 01 February 2008. Available at: http://protect.gost.ru/document.aspx?control=7& id=129018 (accessed 12 September 2019) (in Russian).

4. State Standard 27002-2012. Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Sistemy Menedzhmenta Informatsionnoi Bezopasnosti. Svod Norm I Pravil Menedzhmenta Informatsionnoi Bezopasnosti [Information Technology. Security Techniques. Information Security Management Systems. Code of Practice for Information Security Management]. *FSUE «Standartinform» Internet Portal*, 01 January 2014. Available at: http://protect.gost.ru/document.aspx?control=7&id=183918 (accessed 12 September 2019) (in Russian).

5. State Standard 27003-2012. Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Sistemy Menedzhmenta Informatsionnoi Bezopasnosti. Rukovodstvo Po Realizatsii Sistemy Menedzhmenta Informatsionnoi Bezopasnosti [Information Technology. Security Techniques. Information Security Management Systems. Implementation Guidance of Information Security

Management System]. *FSUE «Standartinform» Internet Portal*, 01 December 2013. Available at: http://protect.gost.ru/document.aspx?control=7&id=183599 (accessed 12 September 2019) (in Russian).

6. State Standard 27004-2011 Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Izmereniia [Information Technology. Security techniques. Information Security Management. Measurement]. *FSUE «Standartinform» Internet Portal*, 01 January 2012. Available at: http://protect.gost.ru/document.aspx? control=7&id=179060 (accessed 12 September 2019) (in Russian).

7. State Standard 27005-2010. Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Menedzhment Riska Informatsionnoi Bezopasnosti [Information Technology. Security Techniques. Information Security Risk Management]. *FSUE «Standartinform» Internet Portal*, 01 December 2011. Available at: http://protect.gost.ru/document.aspx?control=7&id=177398 (accessed 12 September 2019) (in Russian).

8. ISO/IEC 27000:2018(E). Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. *International Organization for Standardization Internet Portal*, 01 February 2018. Available at: https://www.iso.org/ru/standard/73906.html (accessed 12 September 2019).

9. ISO/IEC 27001:2013(E). Information technology – Security techniques – Information security management systems – Requirements. *International Organization for Standardization Internet Portal*, 01 October 2013. Available at: https://www.iso.org/ru/standard/54534.html (accessed 12 September 2019).

10. ISO/IEC 27002:2013(E). Information Technology – Security Techniques – Code of Practice for Information Security Controls. *International Organization for Standardization Internet Portal*, 01 October 2013. Available at: https://www.iso.org/ru/standard/54533.html (accessed 12 September 2019).

11. ISO/IEC 27003:2017(E). Information Technology – Security Techniques – Information Security Management System Implementation Guidance. *International Organization for Standardization Internet Portal*, 01 March 2017. Available at: https://www.iso.org/standard/63417.html (accessed 12 September 2019).

12. ISO/IEC 27004:2016(E). Information technology – Security techniques – Information security management – Measurement. *International Organization for Standardization Internet Portal*, 01 December 2016. Available at: https://www.iso.org/standard/64120.html (accessed 12 September 2019).

13. ISO/IEC 27005:2018(E). Information Technology – Security Techniques – Information Security Risk Management. *International Organization for Standardization Internet Portal*, 01 July 2018. Available at: https://www.iso.org/ru/standard/75281.html (accessed 12 September 2019).

14. Klimov S. M., Sychev M. P. Poster Polygon for Training and Testing Facilities in the Field of Information Security. *Information Counteraction to the Terrorism Threats*, 2015, no. 24, pp. 206-213 (in Russian).

15. Klimov S. M. Imitating Models of Testing the Critically Important Information Objects in the Conditions Of Computer Attacks. *Izvestiya SFedU. Engineering Sciences*, 2016, vol. 181, no. 8, pp. 27-36 (in Russian).

16. Klimov S. M., Zorin E. F., Polovnikov A. Yu., Antonov S. G. Main Directions of Ensuring Information Security of Strategic Missile Systems in Terms of Informational-and-Technical Influences. *Military Thought*, 2016, no. 8, pp. 24-29. (in Russian).

17. Shevyrev A. V., Nevzorov Yu. V., Pimenov P. N., Fomina I. A., Pronin S. A. The Analysis of Stable Functioning a New Generation Robotic Systems In Man-Made Ultrashort Electromagnetic Pulses. *Izvestiya SFedU. Engineering Sciences*, 2016, no. 2 (175), pp. 240-251 (in Russian).

18. Tikhonov R. I., Bubenshchikov Yu. N. The Practice of Testing Units with Unmanned Flying Vehicles Exposed to Information-technical Influence. *Military Thought*, 2019, no. 6, pp. 118-124. (in Russian).

19. Makarenko S. I. *Audit Bezopasnosti Kriticheskoi Infrastruktury Spetsialnymi Informatsionnymi Vozdeistviiami* [Security Audit of Critical Infrastructure with Special Information Impacts]. St. Petersburg, Naukoemkie Tekhnologii Publ., 2018. 122 p. Available at: http://sccs.intelgr.com/editors/ Makarenko/makarenko-audit_ib_2018.pdf (accessed 12 September 2019) (in Russian).

20. Trebovaniia Po Obespecheniiu Bezopasnosti Znachimykh Obektov Kriticheskoi Informatsionnoi Infrastruktury Rossiiskoi Federatsii [Requirements for Ensuring the Security of Significant Objects of Critical Information Infrastructure of the Russian Federation]. *Federal Service for Technical and Export Control of Russia (FSTEC) Internet Portal*, 25 December 2017. Available at: https://fstec.ru/component/attachments/ download/1879 (accessed 12 September 2019) (in Russian).

21. Zabegalin E. V. A Question of Definition of the Term «Information and Technical Impact». *Systems of Control, Communication and Security*, 2018, no. 2, pp. 121–150. Available at: http://sccs.intelgr.com/archive/2018-02/08-Zabegalin.pdf (accessed 12 September 2019) (in Russian).

22. Barishpolets V. A. Informatsionno-Psikhologicheskaia Bezopasnost: Osnovnye-Polozheniia [Information and Psychological Security: Key Points]. *Radioelektronika. Nanosistemy. Informatsionnye tekhnologii*, 2013, vol. 5, no. 2, pp. 62-104.

23. Morozov A. V. *Delovaia Psikhologiia* [Business Psychology]. St. Petersburg, Soyuz Publ., 2000, 576 p. (in Russian).

24. State Standard 13335-1-2006. Informatsionnaia Tekhnologiia. Metody I Sredstva Obespecheniia Bezopasnosti. Chast 1. Kontseptsiia I Modeli Menedzhmenta Bezopasnosti Informatsionnykh I Telekommunikatsionnykh Tekhnologii [Information Technology. Security Methods and Tools. Part 1. Concept and Models of Security Management of Information and Telecommunication Technologies]. *FSUE «Standartinform» Internet-portal*, 01 June 2007. Available at: http://protect.gost.ru/document1.aspx?control=31&id=128738 (accessed 12 September 2019) (in Russian).

25. Repin V. V., Eliferov V. G. *Protsessnyi Podkhod K Upravleniiu. Modelirovanie Biznes-Protsessov* [The Process Approach to Management. Modeling Business Processes.]. Moscow, Mann Ivanov Ferber Publ., 2013, 544 p. (in Russian).

26. Gorchakov L. V., Stas A. N. *Osnovy Iskusstvennogo Intellekta* [The Basics of Artificial Intelligence]. Tomsk, Tomsk State Pedagogical University Publ., 2006, 199 p. Available at: http://koi.tspu.ru/koi_books/gorchakov5/Index.html (accessed 12 September 2019) (in Russian).

27. State Standard 20911–89. Tekhnicheskaia Diagnostika. Terminy I Opredeleniia [Technical Diagnostics. Terms and Definitions]. *FSUE «Standartinform» Internet Portal*, 01 June 2007. Available at: http://protect.gost.ru/document.aspx?control=7&id=138613 (accessed 12 September 2019) (in Russian).

28. Buzov G. A. *Zashchita Informatsii Ogranichennogo Dostupa Ot Utechki Po Tekhnicheskim Kanalam* [Protection of Restricted Access Information from Leakage Through Technical Channels]. Moscow, Goriachaia Liniia - Telekom Publ., 2017. 586 p. (in Russian).

29. Ignatenkov V. G., Sakhnin A. A. *Zashchishchennoe Informatsionnoe Prostranstvo. Kompleksnyi Tekhnicheskii Kontrol Radioelektronnykh Sredstv* [Integrated Technical Control of Electronic Equipment]. Moscow, Goriachaia Liniia - Telekom Publ., 2016. 336 p. (in Russian).

30. Sistema Kontrolia Zashchishchennosti i Sootvetstviia Standartam «Max Patrol» [Security and Compliance Monitoring System «Max Patrol»]. *Positive Technologies Company Internet Portal*, 2018. Available at: https://www.ptsecurity.com/ upload/corporate/ru-ru/products/mp8/PT-MaxPatrol-Data-Sheet-rus.pdf (accessed 12 September 2019) (in Russian).

31. Kompleksnoe Reshenie Dlia Audita Bezopasnosti IT-infrastruktury Predpriiatiia (Skaner Bezopasnosti) [Comprehensive Solution for Security Audit of IT Infrastructure of an Enterprise (Security Scanner) «RedCheck»]. *Internet Site of Software Product «RedCheck»*, 2015. Available at: https://www.redcheck.ru/lib/f/buklet.pdf (accessed 12 September 2019) (in Russian).

32. Bogoras A. G., Peskova O. Yu. Methodology for Testing And Assessment of Firewalls. *Izvestiya SFedU. Engineering Sciences*, 2013, no. 12 (149), pp. 148-156 (in Russian).

33. The Open Source Security Testing Methodology Manual (OSSTMM). *The Institute for Security and Open Methodologies (ISECOM) Internet Portal*, 15 December 2010. Available at: http://www.isecom.org/mirror/OSSTMM.3.pdf (accessed 12 September 2019).

34. The Penetration Testing Execution Standard (PTES). *Internet Site of The Penetration Testing Execution Standard*, 30 April 2012. Available at: http://www.pentest-standard.org (accessed 12 September 2019).

35. Murugiah P. Souppaya, Karen A. Scarfone. Technical Guide to Information Security Testing and Assessment. NIST Special Publications 800-115. *The National Institute of Standards and Technology» (NIST) Internet Portal*, 30 September 2008. Available at: https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment (accessed 12 September 2019).

36. The Information System Security Assessment Framework (ISSAF). *«SourceForge» Internet Portal*, 2014. Available at: https://sourceforge.net/projects/isstf/ (accessed 12 September 2019).

37. A Penetration Testing Model. *Bundesamt für Sicherheit in der Informationstechnik (BSI) Internet Portal*, 21 December 2004. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html (accessed 12 September 2019).

38. Metodika Opredeleniia Aktualnykh Ugroz Bezopasnosti Personalnykh Dannykh Pri Ikh Obrabotke V Informatsionnykh Sistemakh Personalnykh Dannykh [Methodology for Determining Current Threats to the Security of Personal Data During Their Processing in Personal Data Information Systems]. *Federal Service for Technical and Export Control of Russia (FSTEC) Internet Portal*, 09 January 2008. Available at: https://fstec.ru/component/attachments/download/290 (accessed 12 September 2019) (in Russian).

39. Bazovaia Model Ugroz Bezopasnosti Personalnykh Dannykh Pri Ikh Obrabotke V Informatsionnykh Sistemakh Personalnykh Dannykh (vypiska) [The Basic Model of Threats to the Security of Personal Data When They are Processed in Personal Data Information Systems (extract)]. *Federal Service for Technical and Export Control of Russia (FSTEC) Internet-portal*, 09 January 2008. Available at: https://fstec.ru/ component/attachments/download/289 (accessed 12 September 2019) (in Russian).

40. Andreev A. G., Kazakov G. V., Korianov V. V. Model Ugroz Informatsionnoi Bezopasnosti Avtomatizirovannoi Sistemy Podgotovki Dannykh Upravleniia Letatelnymi Apparatami I Model Zashchity [Information Security Threats Model of an Automated Aircraft Control Data Preparation System and Protection Model]. *Proceedings of the Russian Universities: Mechanical Engineering*, 2018, no. 6 (699), pp. 86-95. Available at: http://izvuzmash.ru/ articles/1559/1559.pdf (accessed 12 September 2019) (in Russian).

41. State Standard 31010-2011. Menedzhment Riska. Metody Otsenki Riska [Risk Management. Risk Assessment Methods]. *FSUE «Standartinform» Internet Portal*, 01 December 2012. Available at: http://protect.gost.ru/document.aspx?control=7&id=179313 (accessed 12 September 2019) (in Russian).

42. Polozhenie O Litsenzirovanii Deiatelnosti Po Tekhnicheskoi Zashchite Konfidentsialnoi Informatsii [Regulation on the Licensing of Technical Protection of Confidential Information]. *Federal Service for Technical and Export Control of Russia (FSTEC) Internet Portal*, 03 February 2012. Available at: https://fstec.ru/component/attachments/download/148 (accessed 12 September 2019) (in Russian).

Статья поступила 15 сентября 2019 г.

Информация об авторе

Забегалин Евгений Викторович – кандидат технических наук. Старший научный сотрудник. 4 Центральный научно-исследовательский институт

Министерства обороны РФ. Область научных интересов: информационная безопасность. E-mail: ezabex@yandex.ru

Адрес: 141092, Россия, Московская обл., г. Королёв, мкр. Юбилейный, ул. М.К. Тихонравова, д. 29.

The logical model of integrated technical diagnostics of information security of organizations and significant objects of critical information infrastructure

E. V. Zabegalin

Relevance of the problem: *The Doctrine of Information Security of the Russian Federation (DIS) uses a systematic approach to analyse and ensure information security of the country. This approach considers the country's information security as such of its information sphere which has a complex structure described in the DIS. The author deems it relevant to logically project this systematic approach from the top hierarchical level of the country to other hierarchical levels, including the level of organizations and significant objects of critical information infrastructure, in order to effectively implement the provisions of the DIS. Such logical projection should begin with defining the concept of the information sphere (infosphere) of an organization / critical information infrastructure object (Org/CIIOb) and end with the definition of a standard set of measures to ensure the security of the Org/CIIOb infosphere - measures that are fully adequate to the complex structure of the infosphere and many typical threats to its security.* ***The article is aimed*** *at expanding the standard logical model for the corporate information security management system (ISMS) by adding to it integrated technical diagnostics of the security of the Org/CIIOb information sphere. The diagnostics should include the process function of technical testing of infosphere security by dangerous information and technical impacts (ITI) examined by Russian specialists in their publications.* ***Method for solving the problem:*** *first, based on the concept of the country's information sphere defined in the DIS, the concept of the Org/CIIOb infosphere is to be worked out and typical threats to its security are to be systematized, as well as types of corresponding protective measures; then, in accordance to the ISMS standards, a wider logical model for measures ensuring the Org/CIIOb information security as the Org/CIIOb infosphere security is to be elaborated; and then, based on the ideas of Russian experts on the use of the ITI for technical testing of CIIOb security, a logical model for complex technical diagnosis of the Org/CIIOb information security is to be developed, using graphic notations for logic modeling «Value-added Chain Diagram», «Idef0», and a semantic networks notation.* ***The novelty of the solution*** *consists in substantial elaborating of the concept «information sphere of an organization / critical information infrastructure object» as well as in the development of a logical model for possible complex technical diagnosis of the Org/CIIOb information security (security of the infosphere). This model expands the standard logical model for the corporate ISMS.* ***The theoretical significance*** *of the paper lies in the logical projection of the doctrinal concept of the country's information sphere on the level of organizations and significant objects of critical information infrastructure, as well as in the logical modeling of possible complex technical diagnostics of the Org/CIIOb information security (infosphere security).*

Keywords: *information security, information sphere, infosphere, information security management system, technical diagnosis, technical testing, information and technical impact, logical model.*

Information about Author

Evgeniy Viktorovich Zabegalin – Ph.D. of Engineering Sciences. Senior Research Officer. The 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Field of research: information security. E-mail: ezabex@yandex.ru

Address: Russia, 141092, Moskovskaya oblast, Korolev, mkr. Yubileyny, ulica M.K. Tikhonravova, 29.