СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Соловьев С.В.[1], Тарелкин М.А.[2], Текунов В.В.[3], Язов Ю.К.[4]

Аннотация

Цель статьи: *определение основных направлений разработки, состава и структуры перспективного методического обеспечения в части решения задач организации и ведения технической защиты информации в информационных системах.*

Метод: *обобщение и анализ существующего методического обеспечения организации и ведения технической защиты информации от несанкционированного доступа и тенденций его развития в интересах перехода от качественных к количественным процедурам обоснования требований и выбора путей построения систем защиты информации в информационных системах.*

Полученный результат: *определены факторы, обусловливающие необходимость развития методического обеспечения организации и ведения технической защиты информации, в том числе расширение предметной области защиты информации, необходимость перехода к количественным методам, алгоритмам и процедурам оценки возможностей реализации угроз безопасности информации, обоснования требований по технической защите информации и выбора мер и средств защиты в интересах кардинального повышения обоснованности принимаемых решений по защите, в условиях резко возросших объемов данных, сбор, обработка и анализ которых невозможны без применения соответствующих специальных программных средств и комплексов и др. Применительно к задачам категорирования (классификации) информационных систем и обрабатываемой в них информации, прогнозирования уязвимостей и угроз безопасности информации, а также оценки рисков реализации угроз с учетом фактора времени определены состав и структура перспективного методического обеспечения, подлежащего разработке в том числе с применением современных методов теории искусственного интеллекта (машинного обучения, искусственных нейронных сетей), аппарата составных сетей Петри-Маркова, теории риска и др. Отмечено, что внедрение в практику такого методического обеспечения невозможно без создания программных комплексов, автоматизирующих процессы категорирования, классификации, количественных оценок рисков реализации угроз и построения систем защиты информации.*

Научная новизна: *дано систематизированное представление о составе, структуре и тенденциях развития методического обеспечения организации и ведения технической защиты информации при решении задач категорирования информационных систем и защищаемой в них информации, прогнозирования, оценки возможностей и последствий реализации угроз безопасности информации.*

Вклад авторов: *Соловьев С.В. – оценка состояния и исследований перспектив развития методического обеспечения категорирования информационных система и защищаемой в них информации; Тарелкин М.А.- исследование методов прогнозирования угроз безопасности информации и перспективы их применения при ведении банка данных угроз безопасности информации ФСТЭК России; Текунов В.В. – пути построения*

1 Соловьёв Сергей Вениаминович, кандидат технических наук, доцент, заместитель начальника ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» по информационной безопасности, г. Воронеж, Россия. E-mail: solovev@gniii.ru

2 Тарелкин Михаил Андреевич, старший научный сотрудник ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, Россия. E-mail: gniii@fstec.ru

3 Текунов Василий Васильевич, кандидат технических наук, начальник лаборатории ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, Россия. E-mail: gniii@fstec.ru

4 Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник управления ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, Россия. E-mail: yazoff_1946@mail.ru

DOI:10.21681/2311-3456-2023-1-41-57

перспективной системы прогнозирования угроз безопасности информации по результатам мониторинга публикаций о них в сети Internet; Язов Ю.К. – общее руководство, оценка состояния и перспективы развития методического обеспечения оценки рисков реализации угроз безопасности информации.

Ключевые слова: *алгоритм, вероятность, задача защиты, категорирование, методика, модель, оценка возможностей реализации угрозы, угроза безопасности информации, ущерб, риск, прогнозирование.*

DOI:10.21681/2311-3456-2023-1-41-57

Введение

Необходимость развития методического обеспечения организации и ведения технической защиты информации (ТЗИ) сегодня определяется целым рядом факторов, к основным из которых относятся следующие.

1. Существенное расширение предметной области ТЗИ, включающей в себя сведения о совокупности объектов ТЗИ и их характеристиках, о составе и характеристиках угроз безопасности информации, эксплуатируемых при реализации угроз уязвимостях программного и аппаратного обеспечения, о решаемых задачах защиты, подлежащих применению и применяемых мерах, средствах и системах защиты, нормативном, информационном, методическом и программном обеспечении организации и ведения ТЗИ [1].

2. Необходимость перехода от качественных экспертных процедур оценки возможностей реализации угроз безопасности информации, обоснования требований по ТЗИ и выбора мер и средств защиты к количественным методам в интересах кардинального повышения обоснованности оценок и принимаемых решений по ТЗИ.

3. Развитие информационных технологий, в том числе в интересах совершенствования ТЗИ, с существенным изменением состава и содержания решаемых задач защиты, что обусловливает применение новых методических подходов к их решению. Достаточно отметить развитие технологий, направленных на реализацию стратегий обмана (навязывания ложных представлений об атакуемых информационных системах (ИС) путем применения ложных ИС), или технологий, реализуемых SIEM и SOC-системами с выявлением инцидентов безопасности информации в ИС в режиме времени, близком к реальному.

4. Резко возросшие объемы данных, сбор, обработка и анализ которых невозможны без применения соответствующих специальных алгоритмов (например, применяемых в технологии Data Mining). Например, весьма трудоемким сегодня является сбор, обработка и анализ огромных объемов разнородных данных, публикуемых в сети Internet, об уязвимостях программного обеспечения и возможных угрозах безопасности информации, в том числе в интересах прогнозирования возникновения таких угроз в отечественных ИС в краткосрочной перспективе. Это обусловливает необходимость применения методов искусственного интеллекта – машинного обучения, искусственных нейронных сетей, эволюционных вычислений (прежде всего, генетических алгоритмов), нечетких множеств [2 – 7], логико-лингвистического анализа (реляционных языков описания, семантических сетей представления анализируемых процессов и данных) [8] и др.

5. Необходимость аналитического или/и имитационного моделирования многих процессов, анализируемых в ходе организации и ведения ТЗИ, когда без такого моделирования какие-либо решения по защите оказываются не только несостоятельными, но и зачастую невозможными.

Например, без моделирования динамики реализации угроз безопасности информации с учетом фактора времени решения о возможности такой реализации и тем более требования по защите от угроз становятся некорректными, особенно в условиях применения мер защиты, направленных на опережение процессов реализации угроз.

Следует отметить, что развитие методического обеспечения направлено также на совершенствование информационного обеспечения организации и ведения ТЗИ, касающегося не только прогнозирования угроз безопасности информации, но и обоснования требований и изыскания путей построения систем информационного обеспечения деятельности по ТЗИ [9]. Сложность решения задач по ТЗИ с использованием большого объема разнородной информации из различных источников определяют необходимость создания баз и банков данных, реестров, аккумулирующих наиболее востребованную (часто используемую) тематическую информацию по различным направлениям: по характеристикам угроз, объектам защиты и их компонентам, средствам защиты и др.

Для системной разработки таких информационных ресурсов требуется создание соответствующего методического обеспечения.

Также необходимо учитывать и уже сложившуюся практику ТЗИ, в соответствии с которой проводятся следующие виды работ [1]:

1. Категорирование и определение класса защищенности ИС, выявление и категорирование защищаемой информации;

2. Оценка угроз безопасности информации в ИС;

3. Разработка требований к ИС и ее системе защиты информации (СЗИ), разработка, аттестация по требованиям безопасности информации и ввод СЗИ в эксплуатацию;

4. Контроль и мониторинг защищенности ИС в процессе функционирования.

С учетом изложенного при организации и ведении ТЗИ с использованием перспективного методического обеспечения должен решаться широкий круг задач, в том числе:

а) в рамках первого вида работ по ТЗИ – категорирование (классификация) ИС органов власти, предприятий и организаций в интересах решения задач технической защиты обрабатываемой в них информации в целях отнесения ИС к значимым объектам критической информационной инфраструктуры (КИИ), определения требуемых классов защищенности ИС и уровней защищенности ИС персональных данных (ПДн), определения требуемых классов защиты для применяемых в ИС средств защиты и др.;

б) в рамках второго вида работ по ТЗИ:

- прогнозирование возникновения уязвимостей в программном и аппаратном обеспечении ИС, а также создания эксплойтов, которые могут быть использованы для эксплуатации выявленных уязвимостей;
- прогнозирование угроз безопасности информации, обрабатываемой в ИС, с описанием источников угроз, эксплуатируемых уязвимостей и применяемых эксплойтов или вредоносных программ, возможных объектов воздействия и способов (сценариев) реализации угроз;
- оценка возможности реализации угроз в конкретных ИС на сетевом, системном и прикладном системно-технических уровнях[5], а также оценка последствий от реализации угроз, то есть оценка рисков реализации угроз, и далее определение состава и содержания актуальных угроз безопасности информации в ИС;

в) в рамках третьего вида работ по ТЗИ:

- обоснование требований по защите информации от совокупности актуальных угроз как для ИС в целом, так и при необходимости для программных и программно-аппаратных элементов этих ИС, в том числе в части требуемой эффективности защиты по показателям оценки снижения рисков реализации угроз и требуемой эффективности применения мер (средств) защиты;
- разработка эффективных средств защиты информации с учетом требуемой их эффективности;
- выбор целесообразного состава организационных и организационно-технических мер защиты, построение СЗИ с реализацией обоснованных требований;
- оценка эффективности применения мер и средств защиты информации;

г) в рамках четвертого вида работ по ТЗИ – проведение контрольных мероприятий по проверке выполнения установленных требований, выявление и категорирование нарушений безопасности информации в ИС, построение средств и систем контроля, мониторинг безопасности информации, анализ инцидентов информационной безопасности и управление ими и др.

Для решения каждой из этих задач необходимо иметь соответствующее методическое обеспечение. В рамках одной статьи невозможно охватить весь круг задач, решаемых при организации и ведении ТЗИ, поэтому в данной статье рассматриваются только перспективы развития методического обеспечения решения задач *категорирования* ИС и обрабатываемой в них защищаемой информации, *прогнозирования* возникновения уязвимостей и угроз безопасности информации, а также *оценки рисков* реализации угроз.

С учетом изложенного цель написания данной статьи состоит в определении основных направлений разработки, состава и структуры перспективного методического обеспечения решения указанных задач организации и ведения ТЗИ в информационных системах.

1. Оценка состояния и перспективы развития методического обеспечения категорирования информационных систем и обрабатываемой в них информации

Категорирование (определение категории значимости, класса защищенности) ИС органов власти,

5 Методический документ ФСТЭК России «Методика оценки угроз безопасности информации», утвержден 5 февраля 2021 г.

предприятий и организаций и обрабатываемой в них защищаемой информации проводится в интересах дифференциации требований по ТЗИ. При этом в первую очередь решаются вопросы отнесения ИС к значимым объектам КИИ с присвоением одной из трех категорий значимости или, если такая категория не присваивается, то отмены включения их в список значимых объектов КИИ на основании показателей критериев значимости объектов КИИ и их значений, предусмотренных соответствующим перечнем, утвержденным постановлением Правительства Российской Федерации[6].

Для государственных информационных систем (ГИС) в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. №17 и внесенными в него изменениями[7] устанавливается один из трех классов защищенности ГИС в зависимости от значимости обрабатываемой в ней информации и масштаба ИС (федеральный, региональный, объектовый).

Для ИС, в которых обрабатываются персональные данные (ИСПДн), устанавливается один из четырех уровней защищенности персональных данных в соответствии с постановлением Правительства Российской Федерации от 11 ноября 2012 г. №1119. Аналогичным образом может проводиться категорирование по уровням защищенности иной, подлежащей защите информации ограниченного доступа (содержащей сведения, относящиеся, например, к служебной информации, к коммерческой, врачебной и другим видам тайн).

При всей важности указанных документов следует отметить, что в методическом плане их применение обеспечено пока недостаточно. Краткая характеристика состояния методического обеспечения решения задач категорирования ИС при отнесении их к значимым объектам КИИ на примере определения показателей критерия социальной значимости ИС (аналогично обстоят дела и для критериев политической, экономической, экологической значимости и значимости для обеспечения обороны страны, безопасности государства и правопорядка), определения класса защищенности ГИС и требуемого уровня защищенности ПДн, обрабатываемых в ИСПДн приведена в табл. 1. С учетом изложенного сегодня востребованы модели, методики и программные средства автоматизации процессов категорирования, состав и назначение которых приведены на рис. 1.

Следует отметить, что для получения одинаковых результатов категорирования разными специалистами целесообразно, во-первых, разработать методические рекомендации по категорированию ИС и защищаемой информации в них, а во-вторых, стандартизовать модели, алгоритмы и методики, то есть закрепить их в соответствующих государственных стандартах в интересах регламентации решения задач категорирования.

2. Оценка состояния и перспективы развития методического обеспечения прогнозирования возникновения уязвимостей программного обеспечения и угроз безопасности информации в информационных системах

В настоящее время наблюдается лавинообразный рост угроз безопасности информации для ИС практически во всех сферах жизнедеятельности государства и общества и крайне важно осуществлять своевременный прогноз возникновения таких угроз, выявления уязвимостей как в функционирующих, так и в разрабатываемых ИС.

Такое прогнозирование осуществляется во всех ведущих странах мира. Анализ показал, что сегодня развернуты и функционируют более 150 систем прогнозирования угроз безопасности информации в США, Китае, Японии, Англии, Южной Корее, Франции и Германии и т.д. В них применяются весьма разнообразные методические подходы к прогнозированию, начиная от экспертных методов (морфологического анализа, комиссий, Делфи, Кука, дерева целей и др.) и заканчивая методами, основанными на элементах искусственного интеллекта, такими как методы машинного обучения и анализа, искусственных нейронных сетей, выявления семантических и иных связей между субъектами и объектами, имеющими отношение к угрозам безопасности информации, корреляции разнородных данных, методы нечетких суждений (нечетких множеств, нечетких чисел и нечеткой логики), методы эволюционных вычислений (прежде всего, генетические алгоритмы), а также методы регрессии и экстраполяции, построения деревьев (логических моделей) для кластеризации, классификации и корреляции разнородной информации, градиентного бустинга и др.

6 Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

7 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11 февраля 2013 г. №17 и «Изменения, которые вносятся в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах ...», утвержденные приказом ФСТЭК России от 15 февраля 2017 г.

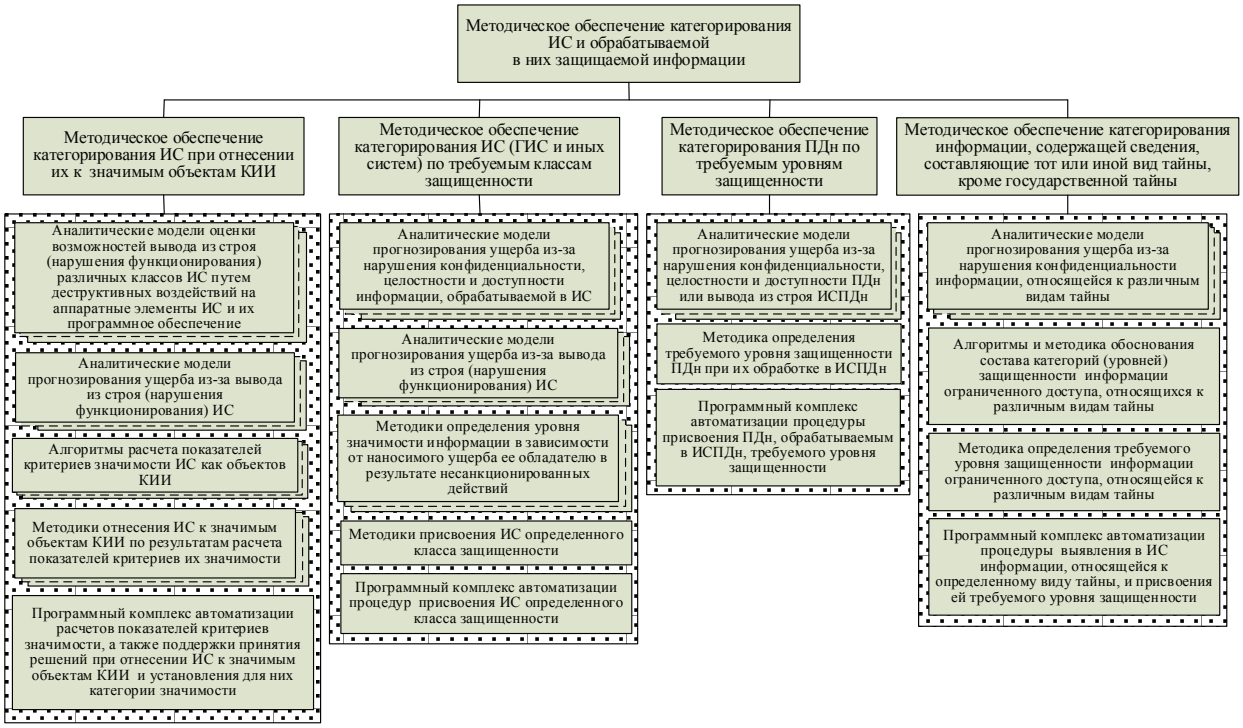

Рис.1. Состав и структура подлежащего разработке методического обеспечения категорирования ИС и обрабатываемой в них защищаемой информации

Таблица 1

Краткая характеристика состояния методического обеспечения категорирования информационных систем

Задача категорирования	Показатель	Состояние развития и недостатки методического обеспечения для определения показателей
Определение категории значимости ИС как возможного объекта КИИ на примере критерия социальной значимости ИС	1. Причинение ущерба жизни и здоровью людей (человек)	Для всех показателей: 1. Определение значения показателя осуществляется экспертно. 2. Оценка значения показателя должна быть прогнозной, в том числе на основе статистических данных, которых сегодня для ИС, являющихся объектами КИИ, практически нет. 3. Методы прогнозирования возможных атак на конкретные ИС и выполнения деструктивных действий отсутствуют (см. раздел 2 данной статьи). 4. Методы, методики, алгоритмы и тем более программные средства автоматизации оценивания показателей, позволяющие спрогнозировать влияние прекращения или нарушений функционирования ИС на возможный ущерб, а также поддержки принятия решений о присвоении категории значимости ИС как объекта КИИ отсутствуют
	2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	
	3. Прекращение или нарушение функционирования объектов транспортной инфраструктуры	
	4. Прекращение или нарушение функционирования сети связи	
	5. Отсутствие доступа к государственной услуге, оцениваемое по максимальном допустимому времени, в течение которого государственная услуга может быть недоступна для ее получателей	
	6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	

Задача категорирования	Показатель	Состояние развития и недостатки методического обеспечения для определения показателей
Определение класса защищенности ГИС (класс определяется двумя показателями: масштабом ГИС и уровнем значимости обрабатываемой информации)	1. Масштаб ГИС (федеральный, региональный, объектовый) определяется в зависимости от того, на какой территории функционирует ГИС	Для предложенного в нормативном правовом документе ФСТЭК России подхода к определению масштаба ГИС какого-либо дополнительного методического обеспечения не требуется
	2. Уровень значимости информации, обрабатываемой в ГИС, определяется в соответствии со степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора в зависимости от того, какой вид нарушений может иметь место (конфиденциальности, целостности или доступности информации)	2.1. Методическое обеспечение прогнозирования возможного ущерба и тем более с разделением ущерба на составляющие, возникающего в результате нарушения конфиденциальности, целостности и доступности защищаемой информации, отсутствует. 2.2. Объемы защищаемой информации в ГИС могут составлять десятки гигабайт. В этом случае весьма сложно составлять даже перечень защищаемой информации, а тем более оценивать возможный ущерб от нарушений ее безопасности. Требуются другие подходы, отличные от изложенного в нормативном правовом документе, для оценки значимости защищаемой информации, например, основанные на теории риска
Определение уровня защищенности персональных данных, обрабатываемых в ИСПДн. Уровень определяется типом выявленных угроз безопасности ПДн	1. Выявление категорий ПДн, которые обрабатываются в ИСПДн.	Выявление категорий ПДн, обрабатываемых в ИСПДн, осуществляется экспертно. Необходимы алгоритмы и реализующие их программные средства категорирования ПДн, построенные с применением элементов искусственного интеллекта
	2. Определение типов угроз безопасности ПДн в ИСПДн.	2.1. Связывать требуемый уровень защищенности ПДн с типом угроз, которые могут быть реализованы, на наш взгляд, некорректно: требуемый уровень защищенности должен достигаться независимо от того, какой состав угроз существует в ИСПдн. Кроме того, состав угроз в современных условиях быстро меняется, в результате при существующем подходе нужно часто менять требуемый уровень защищенности ПДн. 2.2. Тип угрозы в соответствии с постановлением Правительства Российской Федерации №1119 определяется в зависимости от того, имеют место недекларированные возможности в системном (угрозы 1 типа), прикладном (угрозы 2 типа) программном обеспечении ИСПДн, при этом угрозы 3 типа не связываются с наличием указанных недекларированных возможностей. Но недекларированные возможности имеются всегда, а тип угрозы будет определяться тогда тем, сумеет ли обладатель выявить их наличие. Если таковые не выявляются, то это не значит, что они отсутствуют, при этом снижение требуемого уровня защищенности ПДн может иметь весьма негативные последствия. 2.3. Установление типов угроз в ИСПДн сегодня осуществляется только экспертно. Какое-либо методическое обеспечение для этого не разрабатывалось. На наш взгляд, нужно менять подход к определению актуальных угроз безопасности ПДн с ориентацией на применение теории риска и создания соответствующих программных средств для автоматизации процесса определения актуальных угроз
	3. Определение требуемого уровня защищенности ПДн в ИСПДн	Определение требуемого уровня защищенности ПДн на основе установленных категорий ПДн и типов угроз осуществляется достаточно просто и ясно, однако каких-либо обоснований для принятой процедуры такого определения сегодня нет. На наш взгляд, переход к использованию теории рисков и автоматизации процедуры определения требуемого уровня защищенности ПДн, позволит существенно повысить обоснованность требований к уровню защищенности ПДн

В России в интересах обеспечения данными о возможных угрозах безопасности информации в ИС их прогнозирование предполагается осуществлять с использованием банка данных угроз безопасности информации ФСТЭК России (адрес сайта – BDU.fstec.ru). Пока применяются преимущественно экспертные методы прогнозирования. Однако в перспективной системе (рис. 2) предполагается уже на первом этапе ее функционирования, кроме экспертных, применять такие методы, как:

- экстраполяции и регрессии для прогнозирования по ретроспективным данным;
- машинного обучения по ключевым словам для выявления наиболее опасных уязвимостей, способов реализации угроз, реализуемых путем эксплуатации выявленных уязвимостей и применения соответствующих эксплойтов, а также для формирования новых ключевых слов для повышения эффективности поиска новой информации;
- построения и применения искусственных нейронных сетей для распознавания различных текстов, в том числе для использования в семантических анализаторах;
- построения деревьев (логических моделей) для кластеризации, классификации и корреляции разнородной информации, в том числе для построения графов зависимостей исследуемых сущностей (авторов публикаций, хакерских группировок, исследователей уязвимостей), получаемой на этапах мониторинга и предварительной обработки.

Состав и структура требуемого методического обеспечения функционирования такой системы прогнозирования приведен на рис.3. Так же, как и при решении задач категорирования, необходимо разработать и включить в состав методического обеспечения прогнозирования методические рекомендации по прогнозированию и комплекс соответствующих стандартов.

3. Оценка состояния и перспективы развития методического обеспечения оценки рисков реализации угроз безопасности информации

Рассматривая задачу оценки рисков (возможностей и последствий) реализации угроз безопасности информации следует подчеркнуть острую востребо-

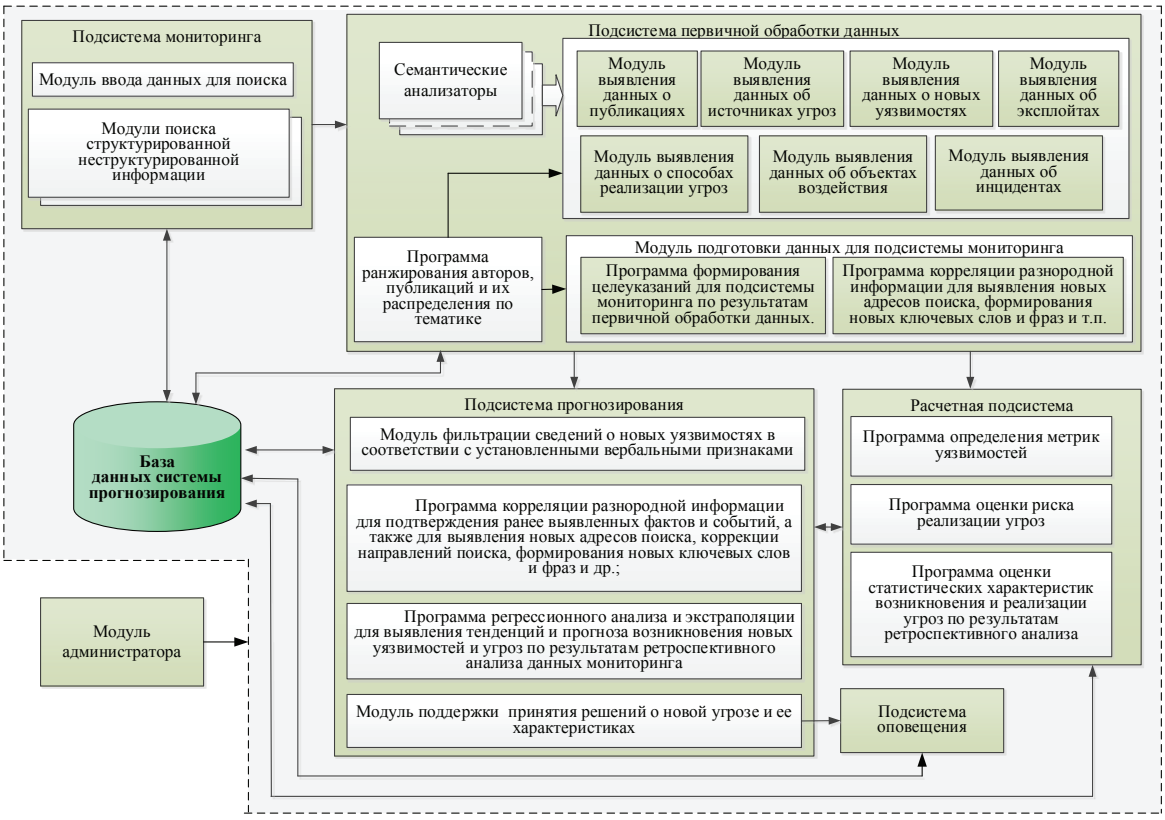

Рис. 2. Состав и структура перспективной системы прогнозирования угроз безопасности информации в отечественных ИС

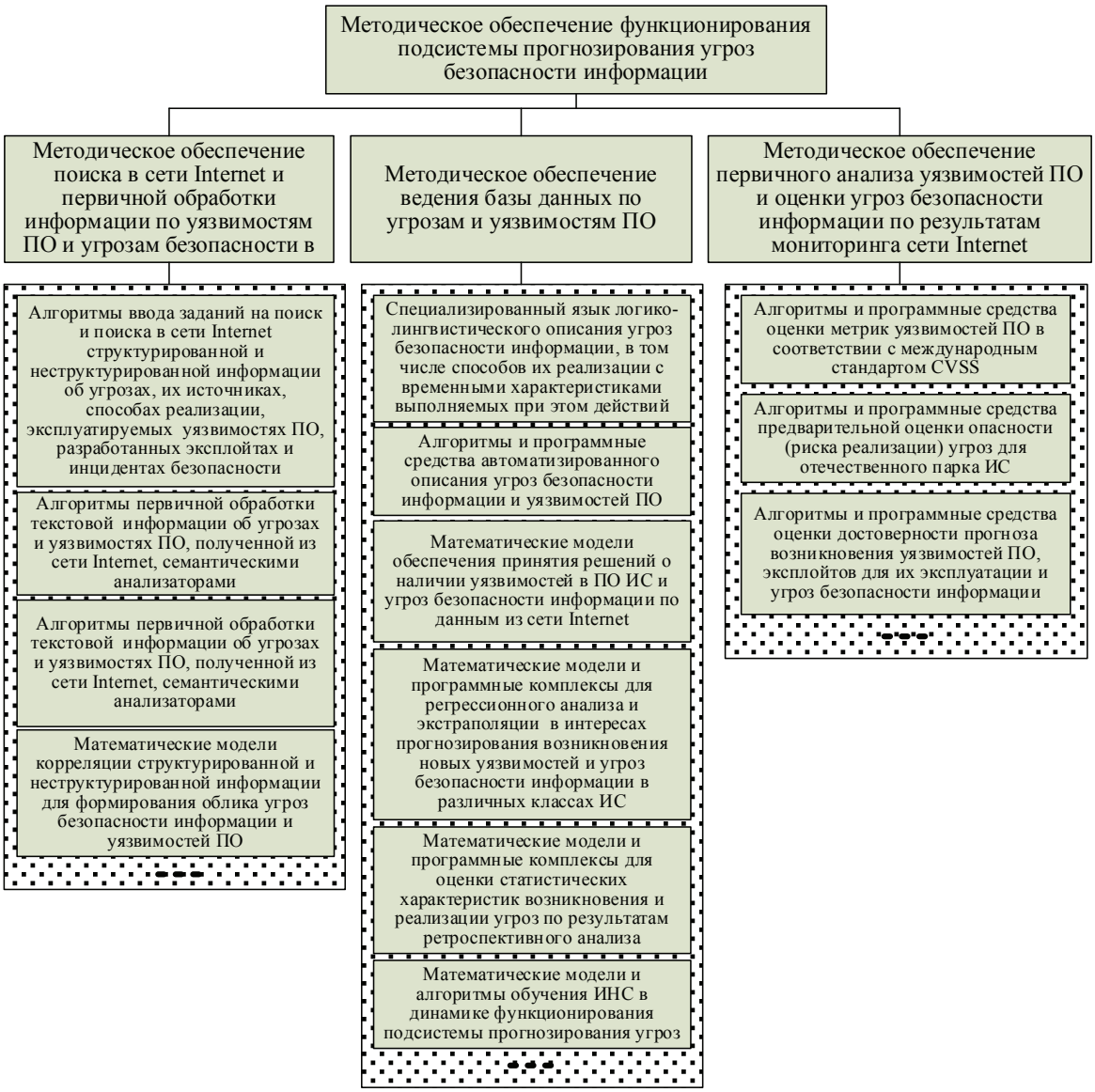

Рис.3. Состав и структура подлежащего разработке методического обеспечения функционирования перспективной системы прогнозирования с использованием сведений банка данных угроз безопасности информации ФСТЭК России

ванность развития методического обеспечения решения этих вопросов.

Сегодня эта задача решается только экспертным путем. При этом в научных публикациях довольно часто звучит призыв перехода к количественным методам анализа угроз безопасности, к учету фактора времени, то есть динамики процессов реализации

С термином «риск» обычно связывалась некая качественная или количественная характеристика, определяющая степень потенциальной опасности некоторого рассматриваемого действия. При этом опасность определялась в виде возможного ущерба от реализации такого действия и оценки возможности этой реализации.

С учетом изложенного до сих пор применялись, по крайней мере, два несколько различающихся подхода к оценке риска.

Первый подход сводится к оценке риска R в виде произведения вероятности $P\left(\zeta_{min} < \zeta \le \zeta_{max}\right)$ того, что при реализации конкретной u -й угрозы будет нанесен ущерб, размеры которого находятся в некотором заданном диапазоне $\left(\zeta_{min}, \zeta_{max}\right)$, и вероятности $P_u(t)$ реализации такой угрозы за заданное время t:

$$R\left(\zeta_{min}, \zeta_{max}, t\right) = P\left(\zeta_{min} < \zeta \le \zeta_{max}\right) \cdot P_u(t). \quad (1)$$

Сложность такого подхода заключается в том, что необходимо иметь плотности распределения вероятностей $w_u(t)$ нанесения ущерба, по которым рассчитываются вероятности нанесения заданных ущербов:

$$\begin{cases} P\left(\zeta_{min} < \zeta \le \zeta_{max}\right) = \int\limits_{\zeta_{min}}^{\zeta_{max}} w_u\left(x\right)dx - \text{при непрерывном законе распределения;} \\ P\left(\zeta_{min} < \zeta \le \zeta_{max}\right) = \sum\limits_{i} \zeta_i \cdot P\left(\zeta_i\right) - \text{при дискретном законе распределения для} \\ \text{всех } i, \text{ для которых } \zeta_{min} < \zeta_i \le \zeta_{max}. \end{cases} \quad (2)$$

Однако как непрерывное, так и дискретное распределение вероятностей нанесения ущерба в подавляющем большинстве случаев неизвестно.

В связи с этим нашел более широкое применение *второй подход*, в котором используется оценка среднего размера $\overline{\zeta_u}$ возможного ущерба, наносимого в результате реализации u-й угрозы, и вероятность $P_u\left(t\right)$ реализации этой угрозы. При этом риск оценивается следующим образом:

$$R_u\left(t\right) = \overline{\zeta_u} \cdot P_u\left(t\right). \quad (3)$$

Однако и в этом случае рассчитать абсолютное значение размер среднего ущерба от реализации угроз в конкретной ИС часто не удается. В связи с этим используется нормированный риск, определяемый следующим образом. Пусть для предприятия (организации) определен предельный ущерб ζ_{lim}, то есть ущерб, недопустимый для данного предприятия, превышение уровня которого исключено. Тогда нормированный риск определяется по формуле:

$$\hat{R}_u\left(t\right) = \frac{\overline{\zeta_u}}{\zeta_{lim}} \cdot P_u\left(t\right) = \beta_u \cdot P_u\left(t\right). \quad (4)$$

Отношение $\beta_u = \overline{\zeta_u} / \zeta_{lim}$ называют индексом ущерба от реализации u-й угрозы [14].

Часто в ходе реализации угрозы выполняется только одно несанкционированное действие относительно объекта воздействия (файла, каталога, директории, аппаратного компонента ИС и т.д.), тогда нормированный риск реализации хотя бы одной из U рассматриваемых угроз рассчитывается следующим образом:

$$\hat{R}_\Sigma\left(t\right) = \frac{1}{\zeta_{lim}} \cdot \sum_{j=1}^{U} C_U^j \cdot \left(\sum_{u=1}^{j} \overline{\zeta_u}\right) \cdot \prod_{u=1}^{j} P_u\left(t\right) \cdot \prod_{k \ne u}^{U} \left[1 - P_k\left(t\right)\right];$$

$$u = \overline{1,U}, j = \overline{1,U}, \quad (5)$$

а если реализуется всё множество рассматриваемых угроз, то по формуле:

$$\hat{R}_\Sigma\left(t\right) = \frac{1}{\zeta_{lim}} \cdot \left(\sum_{u} \overline{\zeta_u}\right) \cdot \prod_{u} \left[P_u\left(t\right)\right]; \; u = \overline{1,U}, \; j = \overline{1,U}. \quad (6)$$

Если же в ходе реализации одной u-й угрозы выполняется некоторый набор действий G_u (например, копирование информации, передача скопированной информации на внешний носитель или по заданному сетевому адресу, а затем уничтожение информации в атакованной ИС), то нормированный риск определяется следующим образом:

$$\hat{R}_u\left(G_u, t\right) = P_u\left(G_u, t\right) \cdot \sum_{g=1}^{G_u} \beta_u^{(g)}, \quad (7)$$

где $\beta_u^{(g)}$ – индекс ущерба от реализации g-го несанкционированного действия ($g = \overline{1, G_u}$) при реализации u-й угрозы; $P_u\left(G_u, t\right)$ – вероятность реализации u-й угрозы в течение времени t с выполнением всей совокупности G_u несанкционированных действий.

В обоих из рассмотренных подходов для оценки риска необходимо определить и вероятность реализации угрозы безопасности информации за заданное время, и размер возможного ущерба.

Учет фактора времени при оценке возможностей реализации угроз по вероятностному показателю связан с необходимостью разработки комплекса соответствующих математических моделей. При этом применение таких моделей без соответствующих программных средств расчета оказывается практически невозможным, что обусловлено как сложностью расчетов, так и большим количеством моделей и необходимых для расчетов исходных данных. Попытки проведения указанных оценок путем их упрощения, отказа от учета динамики реализации угроз неизбежно приводят к некорректным и, как правило, никому не нужным результатам. Более того, оказывается невозможным обоснование применимости мер защиты, направленных на опережение процессов реализации угроз.

Вместе с тем, сегодня для моделирования угроз с учетом фактора времени уже имеется необходимый математический аппарат, позволяющий учитывать фактор времени и оценивать вероятностно-временные характеристики моделируемых процессов. До недавнего времени для аналитического моделирования преимущественно использовался аппарат

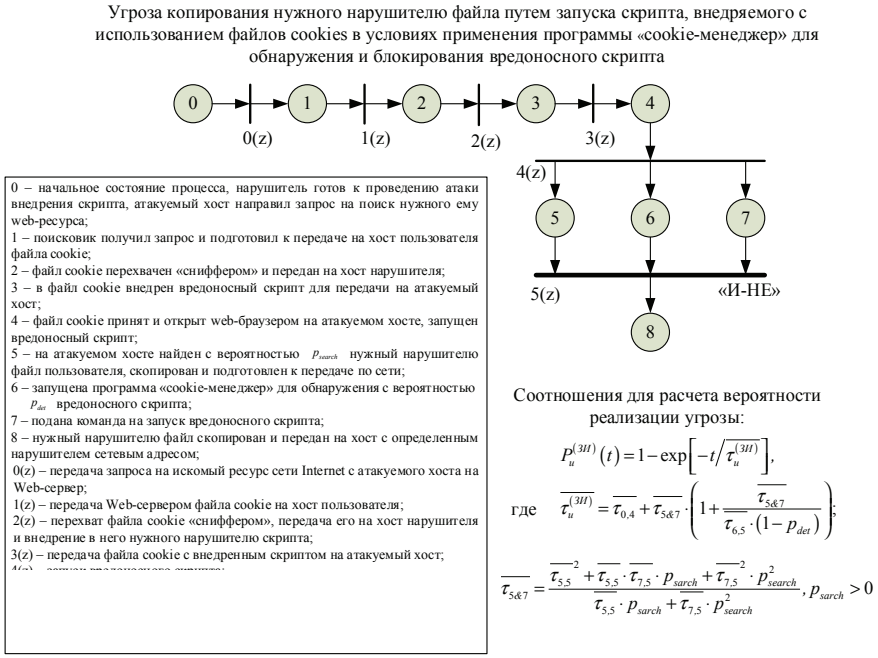

Рис. 4. Граф составной сети Петри-Маркова и соотношения для расчета вероятности реализации угрозы копирования файла путем запуска скрипта, внедряемого с использованием файла cookie, в условиях применения программы «cookie-менеджер» для обнаружения и блокирования вредоносного скрипта

марковских и полумарковских процессов, теория стохастических систем массового обслуживания, теория случайных потоков событий, теория расписаний, аппарат традиционных сетей Петри-Маркова и т.п., а для имитационного моделирования – теория сетей Петри (с разнообразными их модификациями, такими как Е-сети, временные сети, WF-сети, самомодифицируемые сети, ингибиторные сети и др.) и компьютерное моделирование. Если имитационное и компьютерное моделирование угроз безопасности информации пока применяются редко, так как они являются весьма трудоемкими даже для одной угрозы, а для множества угроз – вообще неприемлемыми, то аналитическое моделирование весьма востребовано практикой. Однако применение указанных выше методов аналитического моделирования оказывается проблематичным, если имеются логические условия выполнения моделируемого процесса реализации угрозы, например, условия пропозициональной логики типа «И», «ИЛИ», «И-ИЛИ», «И-НЕ» и др. А такие условия имеют место при моделировании многих угроз, особенно когда реализация угрозы рассматривается при применении мер (средств) защиты. Парирование этой сложности стало возможным с применением разработанного аппарата составных сетей Петри-Маркова [14, 15]. Пример применения такого аппарата для расчета вероятности реализации угрозы безопасности информации приведен на рис. 4.

Вместе с тем построение указанных моделей с применением аппарата составных сетей Петри-Маркова оказывается достаточно сложной процедурой, что обусловливает необходимость создания банка математических моделей процессов реализации угроз с учетом фактора времени и комплекса программных средств, позволяющих в интерактивном режиме вводить необходимые исходные данные, касающиеся характеристик ИС, для которой осуществляются расчеты, сведения об оцениваемых угрозах безопасности информации и выбираемых мерах защиты, затем получать аналитические и графические зависимости показателей оценки возможностей реализации угроз.

Более сложной оказывается проблема оценки ущербов от реализации угроз безопасности информации. Ущерб возникает в результате нарушения конфиденциальности, целостности или доступности информации, относящейся либо к пользовательской, либо к системной. По степени опосредованности различают ущерб, наносимый непосредственно самой защищаемой информации (информационный ущерб), и опосредованный ущерб, обусловленный возникающими последствиями от реализации угроз, включающий в себя финансовый, материальный, экологический,

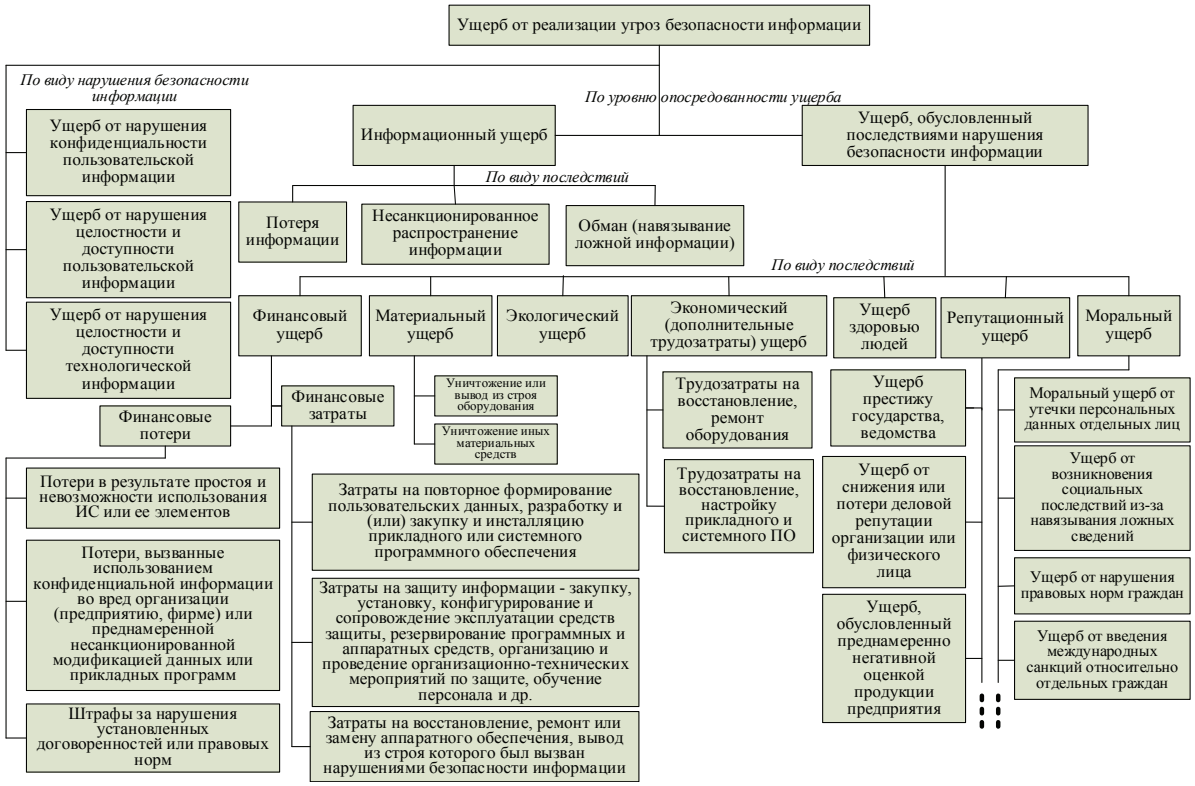

Рис. 5. Классификация ущербов от реализации угроз безопасности информации

экономический, репутационный, моральный ущербы и ущерб здоровью людей (рис. 5).

Рассматривая *информационный ущерб*, необходимо отметить, что предлагалось достаточно много подходов к его оценке [14], например, на основе определения относительного объема или ценности информации, подвергшейся воздействию в результате реализации угрозы, с использованием элементов теории информации К. Шеннона с расчетом изменения энтропии в результате снижения неопределенности информации у пользователя при применении мер защиты и др.

Однако указанные методы оценки информационного ущерба пока не находят какого-либо значимого применения в области защиты информации. Это во многом объясняется сложностью увязки такой оценки с содержанием угроз безопасности информации и преимущественным использованием экспертных процедур.

Рассматривая методы оценки *финансового ущерба*, необходимо отметить, что такие оценки, как правило, являются апостериорными, то есть проводимыми после реализации угроз безопасности информации, а не прогнозными, что востребовано практикой защиты информации. Это обусловлено и отсутствием корректной увязки финансовых потерь с содержанием информации, подвергшейся воздействию в ходе реализации угроз.

Что касается *материального, экономического, экологического ущерба, ущерба здоровью, репутационного* и тем более морального *ущербов,* то методики их корректной оценки и прогноза пока отсутствует.

Весьма проблематичной в связи с изложенным является оценка ущерба от нарушения конфиденциальности информации, поскольку такой ущерб зависит от того, кто и каким образом воспользуется такой информацией во вред государству, организации, владеющей этой информацией, или во вред конкретной личности, через какое время будет использована информация ограниченного доступа и др.

Пока в настоящее время как в России, так и особенно за рубежом применяется балльный метод оценки ущерба от реализации угроз безопасности информации, однако он, во-первых, практически не увязывается с динамикой реализации угроз, а во-вторых, при его использовании весьма сложно перейти к оценкам суммарного ущерба от реализации угроз безопасности информации. Вместе с тем еще в 2006 г. была предложена так называемая универсальная шкала оценок ущербов в интересах совер-

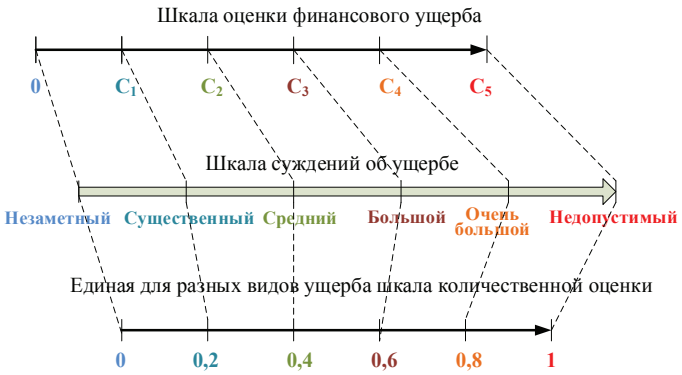

Рис. 6. Пример приведения шкалы оценки финансового ущерба к единой количественной шкале

шенствования балльного метода[8] и подход к оценке с ее использованием относительного риска реализации угроз. При этом было показано, что наиболее приемлемыми для количественной оценки ущербов являются так называемые оппозиционные (полярные) шкалы. Это обусловлено тем, что оппозиционные шкалы основаны на установлении, по крайней мере, двух противоположных (в этом смысле полярных) точек на шкале, определяющих крайние противоположные результаты оценки ущерба (например, отсутствие ущерба и неприемлемый ущерб). Следует подчеркнуть, что особенность шкалы с верхней границей в виде неприемлемого ущерба заключается, прежде всего, в ее универсальности относительно видов ущерба. Однако, она является условной, поскольку ее верхняя граница обусловлена суждением *о неприемлемости ущерба для обладателя информации*.

Сначала строится вербальная шкала оценок ущерба. Наиболее часто при этом используют семь градаций оценок путем задания показателя C с двумя промежуточными лингвистическими оценками – положительной C^+ и отрицательной — C^-, а также двумя оценками, усиленными с помощью модификатора v – vC^+ (например, модификатор может иметь значение «очень» или «неприемлемо большой») и vC^- (модификатор может иметь значение «очень», «несущественный» и т.п.), таких, что $C^+ \le vC^+, C^- \ge vC^-$ и двумя оценками, ослабленными с помощью модификатора w (например, модификатора «скорее») wC^+ и wC^- таких, что $C^+ \ge wC^+$, $C^- \prec wC^-$, а также нейтральной (средней) оценкой C^0. Градации вербальной шкалы упорядочены следующим образом: $vC^- \le C^- \le wC^0 \le wC^+ \le C^+ \le vC^+$ [14].

После построения базовой вербальной шкалы устанавливается ее соответствие каждой из шкал оценок разнородных ущербов. Это позволяет перевести оценки разнородных ущербов в единую шкалу оценок. Затем базовой вербальной шкале ставится в соответствие замкнутый отрезок [0,1], на который проецируется вербальная шкала, пример проекции приведен на рис. 6.

По предложенной универсальной шкале может быть оценен ущерб от выполнения как каждого несанкционированного действия, так и совокупности таких действий, выполняемых при реализации множества угроз безопасности информации.

Однако следует отметить, что сумма ущербов разного вида при реализации совокупности угроз может значительно превышать предельно допустимый уровень.

Пусть относительно i-го блока защищаемой информации ($i \in I$) может быть выполнено множество $G_i = \{g_i\}$ несанкционированных действий (например, файл сначала копируется, а затем уничтожается), каждое из которых может принести определенный ущерб, оцениваемый по универсальной шкале.

Такая оценка представляет собой по сути индекс этого ущерба. Тогда суммарный ущерб при воздействии на i-й блок защищаемой информации оценивается следующим образом:

$$\beta_{iG_i} = \begin{cases} 1, \text{ если } \sum\limits_{g \in G_i} \beta_{ig} \ge 1, g = \overline{1,\ G_i}\ ; \\ \sum\limits_{g \in G_i} \beta_{ig}, \text{если } \sum\limits_{g \in G_i} \beta_{ig} < 1, \end{cases} \quad (8)$$

где β_{ig} — индекс ущерба от реализации g-го деструктивного действия относительно i-го блока защищаемой информации;

G_i — мощность множества несанкционированных действий, которые могут быть выполнены относительно i-го блока информации.

8 Язов, Ю.К. Основы методологии оценки эффективности защиты информации в компьютерных системах / Ю.К. Язов // Ростов-на-Дону: изд-во СКНЦ ВШ, 2006. 274 с.: с илл.

Для всех блоков защищаемой информации, относительно которых возможна реализация угрозы и выполнение всего множества несанкционированных действий, индекс суммарного ущерба определяется аналогично.

Для определения суммарного индекса совокупности разнородных ущербов обладателю может потребоваться учесть разное восприятие им разнородных ущербов. В этом случае следует учесть важность для обладателя разных видов ущерба соответствующим коэффициентом важности V_ϑ вида ущерба ϑ, при этом:

$$\sum_{\vartheta\in\Theta} V_\vartheta = 1, \vartheta = \overline{1,} \qquad (9)$$

где $[\![\Theta]\!]$ — мощность множества видов ущербов (количество видов ущербов). Тогда суммарный ущерб с учетом важности видов ущерба оценивается сверткой:

$$\beta_\Sigma = \sum_{\vartheta\in\Theta} V_\vartheta \cdot \beta_{IG}^{(\vartheta)}, \qquad (10)$$

$\beta_{IG}^{(\vartheta)}$ — индекс суммы ущербов ϑ -го вида при выполнения совокупности G несанкционированных действий относительно множества I защищаемых блоков информации.

Следует подчеркнуть, что при изложенном подходе к оценке ущерба от реализации угроз безопасности информации в ИС пока невозможно полностью исключить экспертный подход, так как необходимо экспертным путем определять, какой из ущербов относится к незаметному, существенному, среднему, большому, очень большому и недопустимому. Для этого нужна система соответствующих правил, которые будут различны для разных видов ущерба и разной защищаемой информации (например, для прикладных программ, персональных данных, информации, составляющей коммерческую тайну и т.д.)[9].

С учетом изложенного перспективы развития методического обеспечения, необходимого для оценки рисков реализации угроз безопасности информации в ИС, приведены на рис. 7.

Так же, как и при решении задач категорирования и прогнозирования, необходимо разработать и включить в состав методического обеспечения оценки рисков реализации угроз методические рекомендации по оценке рисков и комплекс соответствующих стандартов, регламентирующие применяемые при оценке рисков критерии, показатели, методы, алгоритмы и процедуры расчета.

9 В рамках настоящей статьи не рассматриваются состояние и перспективы развития методического обеспечения ТЗИ, содержащей сведения, составляющие государственную тайну.

Заключение

1. Рассмотрены перспективы развития методического обеспечения организации и ведения ТЗИ в части, касающейся решения задач категорирования ИС и обрабатываемой в них защищаемой информации, прогнозирования возникновения уязвимостей и угроз безопасности информации, а также оценки рисков реализации угроз. Показано, что основной тенденцией такого развития является переход от качественных к количественным методам. Однако из-за больших объемов данных и сложности применяемых алгоритмов внедрение в практику количественных методов возможно только путем создания программных комплексов, обеспечивающих автоматизацию решения задач по ТЗИ.

2. Основными направлениями развития методического обеспечения категорирования ИС и обрабатываемой в них информации является создание аналитических моделей, методик и программных комплексов для решения задач количественного обоснования отнесения ИС к значимым объектам КИИ, к классам защищенности, а также обоснования требуемых уровней защищенности персональных данных и иной информации ограниченного доступа, содержащей сведения, составляющие тот или иной вид тайны.

3. Определены состав и структура системы (программного комплекса) прогнозирования угроз безопасности информации в отечественных ИС с широким применением современных методов поиска и анализа информации в сети Internet, реализуемых в семантических анализаторах, в том числе методов искусственного интеллекта, таких как машинное обучение, искусственное нейронные сети, нечеткие множества, эволюционные вычисления (генетические алгоритмы). Это позволит перейти от применяемых сегодня преимущественно экспертных методов к автоматизированным процедурам поиска и анализа необходимых сведений и таким образом существенно повысить эффективность прогноза.

4. Важным направлением совершенствования методического обеспечения организации и ведения ТЗИ является разработка математических моделей, программных комплексов и методических рекомендаций для количественной оценки возможных рисков реализации угроз безопасности информации. Показано, что совершенствование такого обеспечения связано, прежде всего, с созданием комплекса моделей динамики реализации угроз в ИС, позволяющих учесть фактор времени и различные логические условия, имеющие место в процессах реализации угроз, а также с построением универсальной шкалы оценок

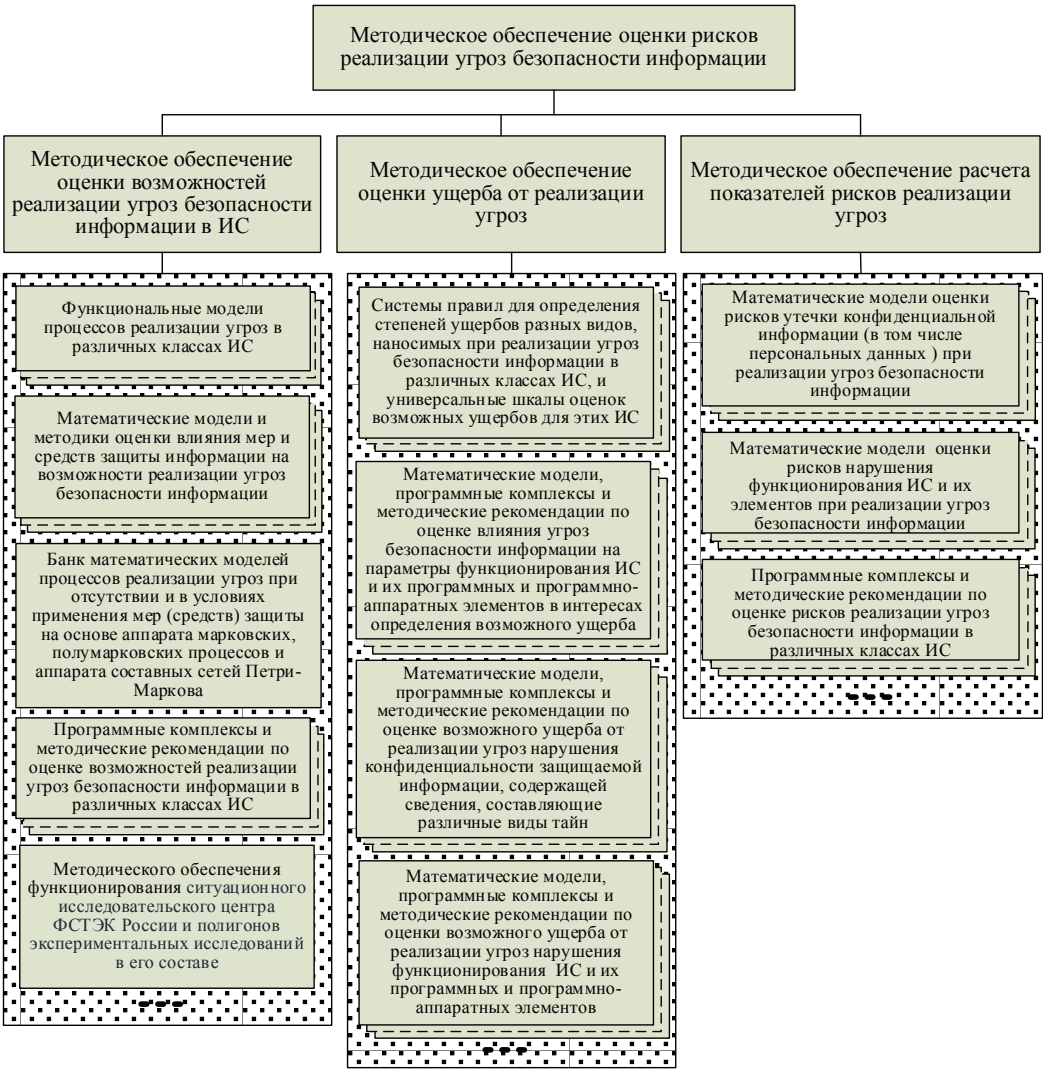

Рис. 7. Состав и структура подлежащего разработке методического обеспечения оценки рисков реализации угроз безопасности информации в информационных системах

ущербов всех видов на основе парадигмы предельного ущерба. Это позволяет количественно оценивать ущербы, складывать ущербы различных видов и далее с учетом динамики реализации угроз оценивать возможные риски.

5. Состав методического обеспечения, необходимого для организации и ведения ТЗИ, несомненно, подлежит уточнению и, возможно, расширению в ходе разработки соответствующих моделей, алгоритмов и процедур. Вместе с тем направления его развития, приведенные в данной статье, на наш взгляд, сохранятся.

Литература

1. Язов, Ю. К., Соловьев, С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография/ Ю. К. Язов, С.В. Соловьев // Воронеж: Кварта, 2018. – 588 с.
2. Павлычев, А.В., Стародубов, М.И., Галимов, А.Д. Использование алгоритма машинного обучения Rabdom Forest для выявления сложных компьютерных инцидентов/ А.В. Павлычев, М.И. Стародубов, А.Д. Галимов // Вопросы кибербезопасности. 2022 г. №5(51). С. 74 – 81. DOI:10.21681/2311-3456-2022-5-74-81.
3. Саенко, И.Б., Котенко, И.В., Аль-Бари, М.Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных / И.Б. Саенко, И.В. Котенко, М.Х. Аль-Бари // Вопросы кибербезопасности. 2022 г. №2(48). С. 87 – 97. DOI:10.21681/2311-3456-2022-2-87-97.

4. Васильев, В.И., Вульфин, А.М., Кучкарова, Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии text mining / В.И. Васильев, А.М. Вульфин, Н.В. Кучкарова // Вопросы кибербезопасности. 2020. №4 (38). С. 22 – 31. DOI 10.21681/ 2311-3456-2020-04-22-31.
5. Котенко, И.В., Саенко, И.Б, Чечулин, А.А. Интеллектуальные сервисы защиты информации в критических инфраструктурах / И.В. Котенко, И.Б Саенко, А.А. Чечулин под общей ред. И.В. Котенко, И.Б. Саенко // СПБ.: БХВ-Петербург, 2019. 400с. ISBN 978-5-9775-398-5.
6. Дойникова, Е.В., Федорченко, А.В., Котенко, И.В., Новикова, Е.С. Методика оценивания защищенности на основе семантической модели метрик и данных/Е.В. Дойникова, А.В. Федорченко, И.В., Котенко, Е.С. Новикова // Вопросы кибербезопасности. 2021. №1 (41). С. 29 – 40. DOI 10.21681/ 2311-3456-2021-1-29-40.
7. Братченко, А.И. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления/ А.И. Братченко, И.В. Бутусов, А.М. Кобелян, А.А. Романов // Вопросы кибербезопасности. 2019. №2 (29). С. 18-24. DOI:10.21681/2311-3456-2019-1-18-24.
8. Тельнов, В.П. Контекстный поиск как технология извлечения знаний в сети интернет / В.П. Тельнов // Программная инженерия. 2017. Т. 8. № 1. С. 26 – 37. DOI: 10.17587/prin.8.26-37.
9. Язов, Ю.К., Соловьев, С.В., Тарелкин, М.А. Логико-лингвистическое моделирование угроз безопасности информации в информационных системах// Ю.К. Язов, С.В. Соловьев, М.А. Тарелкин // Вопросы кибербезопасности. 2022, №4 (50), с. 13 – 23. DOI:10.21681/2311-3456-2022-4-13-23.
10. Соловьев, С.В. Информационное обеспечение деятельности по технической защите информации/ С.В. Соловьев, Ю.К. Язов // Вопросы кибербезопасности. 2021 г. №1(41). С. 69 – 79. DOI: 10.21681/2311-3456-2021-1-69-79.
11. Госькова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. №2. С. 42-49. DOI:10.21681/2311-3456-2019-2-42-49.
12. Лифшиц, И.И., Зайцева, А.А. Методика оценки рисков безопасности информационных технологий для сложных промышленных объектов в распределенных киберфизических системах/ И.И. Лифшиц, А.А., Зайцева // Информационно-управляющие системы. 2019.том 17, №5. С.51 – 59.
13. Васильев, В.И., Вульфин, А.М., Герасимова, И.Б., Картак, В.М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт / В.И. Васильев, А.М. Вульфин, И.Б. Герасимова, В.М. Картак // Вопросы кибербезопасности. 2020. №2 (36). С. 11-21. DOI:10.21681/2311-3456-2020-2-11-21.
14. Язов, Ю. К., Соловьев, С.В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю. К. Язов, С.В. Соловьев // Санкт-Петербург: Изд-во Наукоемкие технологии, 2023. – 263 с.
15. Язов, Ю.К., Анищенко, А.В. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография / Ю.К. Язов, А.В. Анищенко // Воронеж: Кварта, 2020. – 173 с.

STATUS AND PROSPECTS OF DEVELOPMENT METHODOLOGICAL SUPPORT FOR TECHNICAL PROTECTION OF INFORMATION IN INFORMATION SYSTEMS

Soloviev S.V[10], Tarelkin M.A.[11], Tekunov V.V.[12], Yazov Yu.K.[13],

Abstract

The goal of article *is determine the main areas for development, composition and structure of prospective methodological support for the organization and maintenance of technical protection of information in information systems.*

The method of research: *is summary and analysis the existing methodological support for organization and maintenance of the technical protection of information from unauthorized access and its development trends in the interests of the conversion from qualitative to quantitative procedures of substantiation requirements and selection process to build information security system in information systems.*

10 Sergey V. Soloviev, Ph.D., Associate Professor, Deputy Head of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control, Voronezh, Russia. E-mail:solovev@mail.ru

11 Mikhail A. Tarelkin, Senior Research Associate of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control, Voronezh, Russia. E-mail: gniii@fstec.ru

12 Vasily V. Tekunov, Ph.D., Head of Laboratory of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control, Voronezh, Russia. E-mail gniii@fstec.ru.

13 Yuri K. Yazov, Dr.Sc., Professor, Chief Researcher of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control, Voronezh, Russia. E-mail:yazoff_1946@mail.ru

The result of the research: *The factors defining the need to develop methodological support for the organization and maintenance of technical protection of information have been identified, including subject area extension of information protection, the need to move to quantitative research methods, algorithms and procedures for assessment the possibilities of implementing information security threats, the need to justify the requirements for technical protection of information and select protection measures and means. Data volume has increased dramatically and processes of information gathering and analysis are impossible without the use of corresponding special software tools and complexes. The composition and structure of prospective methodological support have been developed, including using modern methods of artificial intelligence theory (machine learning, artificial neural networks (ANNs)), the apparatus of composite Petri-Markov nets, risk theory, etc., for the tasks of categorizing the information systems and the information processed in them, identifying information security threats and vulnerabilities, as well as threat risk assessment considering time factor. It was noted that the introduction of such support into practice is impossible without the creation of software systems that automate categorization processes, quantitative risk assessments of implementing threats and building information protection systems.*

Scientific novelty: *a systematic idea of the composition, structure and prospects of development methodological support has been identified for the organization and maintenance of technical protection of information to solve problems of categorizing the information systems and the information processed in them, forecasting, assessment the possibilities and consequences of implementing information security threats.*

Author contributions: *Soloviev S.V. — assessment of the status and research of the prospects of development methodological support for the categorization the information system and the information processed in them; Tarelkin M.A. — study of methods of threats forecasting for information security and their prospective applications in the management of the Data Bank of information security threats of FSTEC of Russia; V.V. Tekunov — ways to build a promising system for threat forecasting to information security based on the monitoring publications results about them on the Internet; Yazov Yu.K. — general guidance, assessment of the states and prospects of development methodological support for risk assessment of implementing information security threats.*

Keywords: *algorithm, probability, protection task, categorization, methodology, model, assessment the possibilities of implementing information security threats, information security threats, damage, risk, forecasting.*

References

1. Jazov, Ju. K., Solov'ev, S.V. Organizacija zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija/ Ju. K. Jazov, S.V. Solov'ev // Voronezh: Kvarta, 2018. – 588 s.
2. Pavlychev, A.V., Starodubov, M.I., Galimov, A.D. Ispol'zovanie algoritma mashinnogo obuchenija Rabdom Forest dlja vyjavlenija slozhnyh komp'juternyh incidentov/ A.V. Pavlychev, M.I. Starodubov, A.D. Galimov // Voprosy kiberbezopasnosti. 2022 g. №5(51). S. 74 – 81. DOI:10.21681/2311-3456-2022-5-74-81.
3. Saenko, I.B., Kotenko, I.V., Al'-Bari, M.H. Primenenie iskusstvennyh nejronnyh setej dlja vyjavlenija anomal'nogo povedenija pol'zovatelej centrov obrabotki dannyh / I.B. Saenko, I.V. Kotenko, M.H. Al'-Bari // Voprosy kiberbezopasnosti. 2022 g. №2(48). S. 87 – 97. DOI:10.21681/2311-3456-2022-2-87-97.
4. Vasil'ev, V.I., Vul'fin, A.M., Kuchkarova, N.V. Avtomatizacija analiza ujazvimostej programmnogo obespechenija na osnove tehnologii text mining / V.I. Vasil'ev, A.M. Vul'fin, N.V. Kuchkarova // Voprosy kiberbezopasnosti. 2020. №4 (38). S. 22 – 31. DOI 10.21681/ 2311-3456-2020-04-22-31.
5. Kotenko, I.V., Saenko, I.B, Chechulin, A.A. Intellektual'nye servisy zashhity informacii v kriticheskih infrastrukturah / I.V. Kotenko, I.B Saenko, A.A. Chechulin pod obshhej red. I.V. Kotenko, I.B. Saenko // SPB.: BHV-Peterburg, 2019. 400s. ISBN 978-5-9775-398-5.
6. Dojnikova, E.V., Fedorchenko, A.V., Kotenko, I.V., Novikova, E.S. Metodika ocenivanija zashhishhennosti na osnove semanticheskoj modeli metrik i dannyh/E.V. Dojnikova, A.V. Fedorchenko, I.V., Kotenko, E.S. Novikova // Voprosy kiberbezopasnosti. 2021. №1 (41). S. 29 – 40. DOI 10.21681/ 2311-3456-2021-1-29-40.
7. Bratchenko, A.I. Primenenie metodov teorii nechetkih mnozhestv k ocenke riskov narushenija kriticheski vazhnyh svojstv zashhishhaemyh resursov avtomatizirovannyh sistem upravlenija/ A.I. Bratchenko, I.V. Butusov, A.M. Kobeljan, A.A. Romanov // Voprosy kiberbezopasnosti. 2019. №2 (29). S. 18-24. DOI:10.21681/2311-3456-2019-1-18-24.
8. Tel'nov, V.P. Kontekstnyj poisk kak tehnologija izvlechenija znanij v seti internet / V.P. Tel'nov // Programmnaja inzhenerija. 2017. T. 8. № 1. S. 26 – 37. DOI: 10.17587/prin.8.26-37.
9. Jazov, Ju.K., Solov'ev, S.V., Tarelkin, M.A. Logiko-lingvisticheskoe modelirovanie ugroz bezopasnosti informacii v informacionnyh sistemah// Ju.K. Jazov, S.V. Solov'ev, M.A. Tarelkin // Voprosy kiberbezopasnosti. 2022, №4 (50), s. 13 – 23. DOI:10.21681/2311-3456-2022-4-13-23.
10. Solov'ev, S.V. Informacionnoe obespechenie dejatel'nosti po tehnicheskoj zashhite informacii/ S.V. Solov'ev, Ju.K. Jazov // Voprosy kiberbezopasnosti. 2021 g. №1(41). S. 69 – 79. DOI: 10.21681/2311-3456-2021-1-69-79.

11. Gos'kova D.A., Massel' A.G. Tehnologija analiza kiberugroz i ocenka riskov kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti. 2019. №2. S. 42-49. DOI:10.21681/2311-3456-2019-2-42-49.
12. Lifshic, I.I., Zajceva, A.A. Metodika ocenki riskov bezopasnosti informacionnyh tehnologij dlja slozhnyh promyshlennyh ob#ektov v raspredelennyh kiberfizicheskih sistemah / I.I. Lifshic, A.A., Zajceva // Informacionno-upravljajushhie sistemy. 2019.tom 17, №5. S.51 – 59.
13. Vasil'ev, V.I., Vul'fin, A.M., Gerasimova, I.B., Kartak, V.M. Analiz riskov kiberbezopasnosti s pomoshh'ju nechetkih kognitivnyh kart / V.I. Vasil'ev, A.M. Vul'fin, I.B. Gerasimova, V.M. Kartak // Voprosy kiberbezopasnosti. 2020. №2 (36). S. 11-21. DOI:10.21681/2311-3456-2020-2-11-21.
14. Jazov, Ju. K., Solov'ev, S.V. Metodologija ocenki jeffektivnosti zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju. K. Jazov, S.V. Solov'ev // Sankt-Peterburg: Izd-vo Naukoemkie tehnologii, 2023. – 263 s.
15. Jazov, Ju.K., Anishhenko, A.V. Seti Petri-Markova i ih primenenie dlja modelirovanija processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah: monografija / Ju.K. Jazov, A.V. Anishhenko // Voronezh: Kvarta, 2020. – 173 s.