С.В. Скрыль,
доктор технических наук, профессор;
А.М. Сычев,
кандидат технических наук, доцент;
Т.В. Мещерякова,
кандидат физико-математических наук

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ДАННЫХ В УСЛОВИЯХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ: КОНЦЕПЦИЯ И ВОЗМОЖНОСТИ

ASSESSMENT OF EFFECTIVENESS OF INFORMATIONAL PROCESSES IN THE AUTOMATED SYSTEMS OF DATA PROCESSING IN THE CONDITIONS OF THREATS TO SECURITY OF INFORMATION: CONCEPT AND OPPORTUNITIES

Приводится структуризация методического аппарата для оценки характеристик информационных процессов в автоматизированных системах обработки данных в условиях угроз безопасности информации, а также средства исследования, способствующие реализации целей исследования и обеспечение адекватности оценки исследуемых характеристик.

Structurization of the methodical device for assessment of characteristics of informational processes is given in the automated systems of data processing in the conditions of threats to security of information, and also means of a research, the promoting realization of research objectives and ensuring adequacy of assessment of the studied characteristics.

Исходя из содержания понятия «концепция» (*лат. conceptio*), как определенного способа понимания и трактовки исследуемого явления, сформулируем отдельные положения концепции оценки эффективности информационных процессов в автоматизированных системах обработки данных (АСОД) в условиях угроз безопасности информации. При этом, в качестве исследуемого явления рассматривается комплексное влияние характеристик процессов накопления, обработки и обмена информацией, характеристик угроз ее безопасности и характеристик механизмов защиты информации на эффективность информационных процессов в рассматриваемых условиях. Системологической [1] основой данной концепции служит методология комплексной защиты информации от несанкционированного доступа (НСД).

Концепция оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации имеет как теоретиче-

скую, так и прикладную направленность. Теоретическая направленность проявляется теоретическими основаниями, используемыми в процессе исследования механизмов обработки информации в системах рассматриваемого типа, воздействия угроз безопасности информации и механизмов реагирования на подобного рода угрозы как единого объекта исследования. Прикладная направленность проявляется возможностями адекватной оценки характеристик объекта исследования.

Основополагающими принципами концепции оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации являются принципы дифференцированного исследования объекта и интегрированности методического аппарата [1]. В соответствии с первым принципом предполагается структуризация методического аппарата для оценки характеристик исследуемых процессов, соответствующая декомпозиционной структуре их целевой функции. В соответствии со вторым принципом в единое целое интегрируются направления исследования, методический аппарат, а также средства исследования, способствующие реализации целей исследования и обеспечение адекватности оценки исследуемых характеристик.

Содержание концепции оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации логически вытекает из научно-методологических основ комплексной защиты информации от НСД (рис. 1) и практических направлений их реализации. В [2] комплексная защита информации от НСД определяется как систематизированная совокупность сведений и решений, необходимых и достаточных для изучения, анализа и синтеза систем защиты информации от НСД, решения задач и проблем защиты, возникающих в реальных АСОД в условиях угроз безопасности информации.

Представим основу общей структуры рассматриваемой концепции в виде ряда положений.

1. Формирование структурного представления АСОД с учетом условий ее функционирования. 2. Обоснование системной классификации характеристик эффективности реализации информационных процессов в АСОД, различных вариантов воздействия угроз безопасности информации и механизмов защиты информации от подобного рода угроз.

3. Уточнение (формирование) унифицированной структуры методологического аппарата для исследования информационных процессов в системах рассматриваемого типа, воздействия угроз безопасности информации и процессов реагирования на подобного рода угрозы.

4. Структурирование и представление исследовательской среды.

5. Формирование целей и задач исследования, выбор моделей и методов их решения.

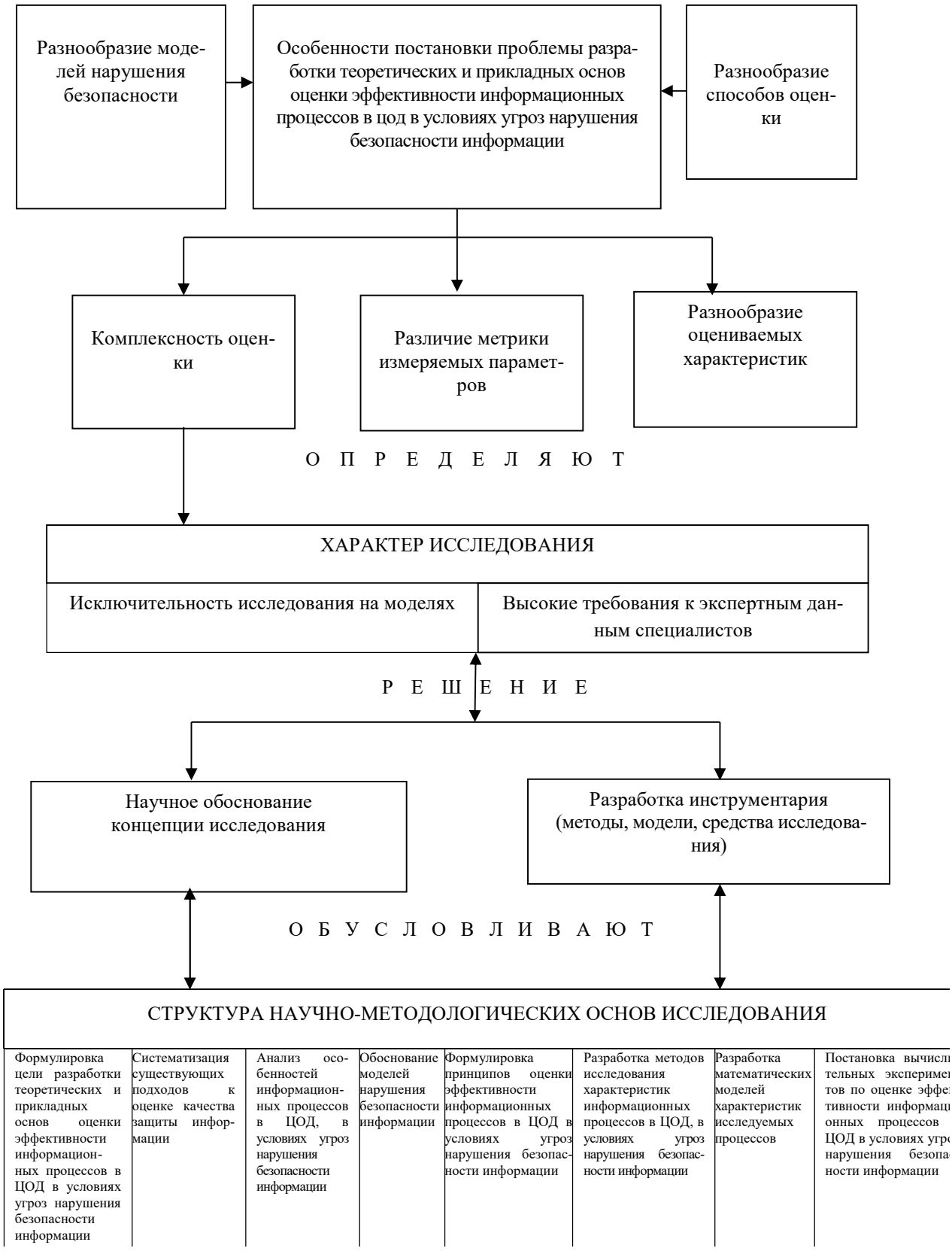

Рис. 1. Содержание научно-методологических основ оценки характеристик информационных процессов в АСОД в условиях угроз безопасности информации

6. Уточнение перечня, классификации и структуры характеристик информационных процессов в АСОД.

7. Классификация и оценка возможных дестабилизирующих факторов, характеристик источников угроз безопасности информации в АСОД, оказывающих влияние на защищенность информации.

8. Выбор инструментальных средств для системных оценок эффективности защиты информации от НСД.

9. Разработка системы концептуальных решений, обеспечивающих оценку эффективности информационных процессов в АСОД в условиях угроз безопасности информации.

10. Формирование системы условий, обеспечивающих практическую реализацию заданных вариантов и стратегий исследования.

С учетом определения понятия «теория» (*греч. theōria*) – исследование, теоретический характер концепции оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации составляет восприятие данной проблемы и как системы основных идей в области информационной безопасности, и как формы научного познания, дающих целостное представление о закономерностях и существенных связях между характеристиками информационных процессов, характеристиками угроз безопасности информации и характеристиками процессов обеспечения ее защиты.

Кроме понятия «теория» основополагающим понятием при формировании концепции оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации является понятие «предмет». Под предметом в рамках рассматриваемой концепции понимается теоретический образ исследуемых процессов. Спецификой предмета в данном случае, как источника знаний о механизмах накопления, обработки и обмена информацией, угрозах ее безопасности и механизмах защиты, является получение знаний не путем непосредственного обращения к этим механизмам, как к объекту исследования, а формальными методами общей теории системного анализа, информатики и теории моделирования систем. При этом предметная область специфицируется фактологическими данными, положенными в основу этих методов, а сами методы формируют вариант интеграции знаний об объекте исследования.

Анализ понятий «теория», «концепция» и «метод» в рамках проблемы оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации позволяет установить соотношения между этими категориями.

В данном контексте понятие «теория» следует рассматривать как совокупность методов получения выводных знаний на основе концептуальных, понятийных и фактологических.

В условиях проблематики исследования информационных процессов в АСОД в условиях угроз безопасности информации рассмотрение мето-

дов, в виде особой формы знаний, и доведения этих знаний до уровня единственной концепции, имеет место совпадение понятий «метод», «теория» и «концепция». При этом компонентами теории как метода формального комбинаторного выведения новых знаний являются известные понятия и концептуальные положения основ информационной безопасности и феноменологические знания, полученные путем анализа закономерностей практики обеспечения защиты информации от НСД.

Исходя из изложенного концепцию оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации следует рассматривать как систему взглядов и идей по исследованию механизмов накопления, обработки и обмена информацией, угроз ее безопасности и механизмов защиты, дающая целостное представление о содержании рассматриваемой проблемы, закономерностях ее развития, существенных связях с другими проблемами в сфере комплексной защиты информации в АСОД, формирующаяся на основе опыта практического решения задач исследования механизмов обеспечения безопасности информации и определяющая направления совершенствования и повышения адекватности оценки.

Концепция оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации преследует следующие цели:

- формирование адекватных сведений о сущности проблемы оценки;
- адекватное отображение структуры и содержания взаимосвязей с другими проблемами в сфере комплексной защиты информации от НСД;
- систематизация опыта исследований в сфере комплексной защиты информации от НСД;
- выбор направлений эффективного решения задач исследования механизмов обеспечения безопасности информации в АСОД и предоставление для этого соответствующих методических средств;
- формирование научно обоснованных перспективных направлений развития теории и практики исследования механизмов обеспечения безопасности информации в АСОД.

Необходимость развития концепции оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации подтверждается следующими объективными предпосылками:

- обоснованием актуальности проблемы адекватности оценки характеристик механизмов накопления, обработки и обмена информацией, угроз ее безопасности и механизмов защиты;
- наличием опыта исследования механизмов обеспечения безопасности информации в АСОД;
- наличием методической базы оценки характеристик механизмов накопления, обработки и обмена информацией, угроз ее безопасности и механизмов защиты в АСОД;

- наличием государственного органа (Федеральной службы по техническому и экспортному контролю) функционально ориентированного на решение проблем оценки защищенности информации;

- наличием определенного количества квалифицированных кадров-профессионалов в области исследования защищенности объектов информатизации;

- выполнением научно-исследовательских и опытно-конструкторских работ, связанных с необходимостью оценки защищенности объектов информатизации;

- разнообразием объектов исследования;

- сложностью реализации оптимальных вариантов оценки, учитывающих многообразие существующих методов и моделей.

Частная постановка соответствующих оптимизационных задач может быть сформулирована в следующем виде: разработать методический аппарат оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации так, чтобы требуемый уровень адекватности оценки обеспечивался минимальной номенклатурой используемых для оценки математических моделей или чтобы при заданной номенклатуре математических моделей достигался максимально возможный уровень адекватности оценки.

Качественная зависимость адекватности (*A*) оценки характеристик механизмов обеспечения безопасности информации в АСОД от номенклатуры (*N*) математических моделей, используемых для оценки при заданном числе уровней (*D*) функциональной декомпозиции исследуемых процессов может быть представлен так, как показано на рис. 2.

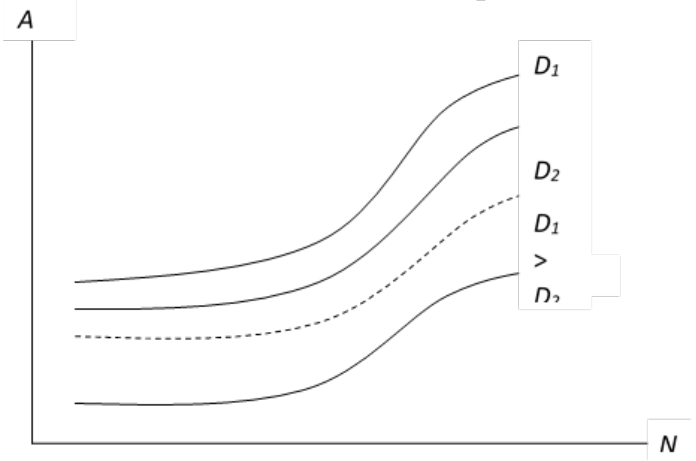

Рис. 2. Качественная зависимость адекватности оценки характеристик механизмов обеспечения безопасности информации в АСОД от номенклатуры математических моделей

Характерным при этом является не только сам факт зависимости адекватности оценки характеристик механизмов обеспечения безопасности информации в АСОД от номенклатуры математических моделей, но также рост этой зависимости при увеличении числа уровней функциональной де-

композиции исследуемых процессов.

Этот пример иллюстрирует необходимость при разработке концепции оценки эффективности информационных процессов в АСОД в условиях угроз безопасности информации детального и всестороннего рассмотрения теоретических аспектов, причем на такой методической основе, которая позволила бы:

- объективно отразить сущность проблемы исследования характеристик информационных процессов в АСОД в условиях угроз безопасности информации;
- обосновать перспективные и наиболее рациональные пути практической реализации концепции;
- системно учитывать совокупности факторов, определяющих адекватность оценки;
- использовать новые математические абстракции при синтезе моделей исследуемых процессов, характерные только процессам обеспечения безопасности информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ЛИТЕРАТУРЫ

1. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений. / С.В. Скрыль, А.А. Шелупанов. – М.: Машиностроение, 2008. – 138 с.

2. Основы информационной безопасности: учебник для высших учебных заведений МВД России / под ред. В.А. Минаева и С.В. Скрыля. – Воронеж: Воронежский институт МВД России, 2001. – 464 с.