Международный опыт правового регулирования информационной безопасности и возможности по его комплексному использованию в Российской Федерации

Аннотация: в статье представлено обобщенное описание международного опыта правового регулирования информационной безопасности и возможности его применения в Российской Федерации. Представлены результаты систематизации международно-правовых норм в сфере информационной безопасности и их соотнесения с международными стандартами информационной безопасности, данные по международному опыту правоприменительной практики в сфере информационной безопасности на основе применения международных стандартов информационной безопасности. Кроме того, в обобщенной форме дано описание информационных отношений в сети Интернет, как инфраструктуры глобального информационного и ноосферных обществ, перспективных международных отношений, а также особенности сетевых информационных угроз. Показана важность использования этого опыта применения современных информационно-аналитических систем для практической реализации процессов информационного обеспечения.

Ключевые слова: международный опыт, правовое регулирование информационной безопасности, моделирование процессов информационной безопасности, аналитические системы анализа правового регулирования информационной безопасности, информационные отношения в глобальной сети Интернет.

По мере развития человечества, при переходе от одного типа общества к другому: *индустриальное — постиндустриальное — информационное — ноосферное* (рис.1) информация и знания становятся ключевым фактором обеспечения конкурентоспособности страны.

Нынешний этап развития информационных технологий характеризуется возможностью массированного информационного воздействия на индивидуальное и общественное сознание вплоть до проведения крупномасштабных информационных войн, в результате чего неизбеж-

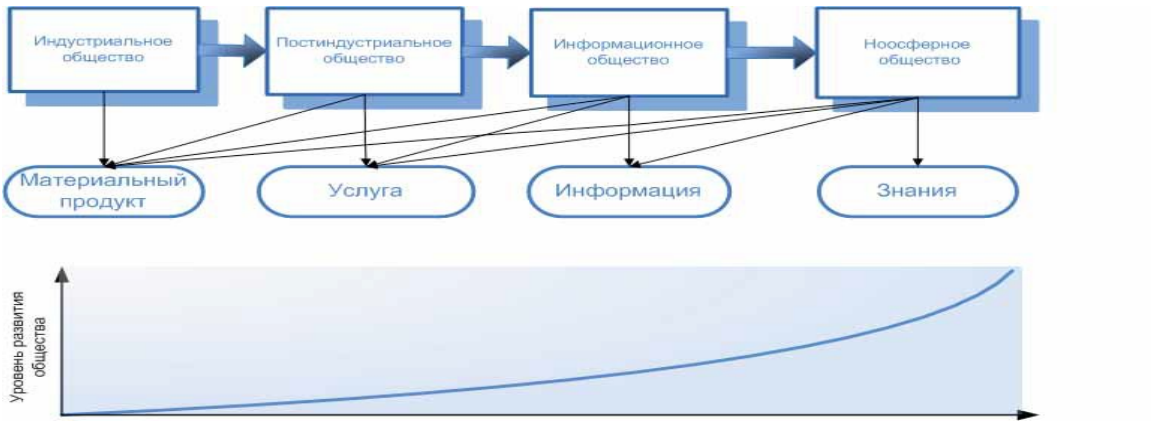

Рис.1. Развитие общества и производственных возможностей человека

ным противовесом принципу свободы информации становится принцип информационной безопасности (ИБ).

Этот принцип обусловлен глобальной информационной революцией, стремительным развитием и повсеместным внедрением новейших информационных технологий и глобальных средств телекоммуникации. Проникая во все сферы жизнедеятельности государств, информационная революция расширяет возможности развития международного сотрудничества, формирует планетарное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса.

Вместе с тем становится очевидным, что наряду с положительными моментами такого процесса создается и реальная угроза использования достижений в информационной сфере с целями, несовместимыми с задачами поддержания мировой стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. Опасным источником угроз является растущая отечественная и международная компьютерная преступность [1-7].

Системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные на укрепление международной информационной безопасности, и вместе с тем максимально учитывались бы национальные интересы.

Международную правовую основу регулирования общественных отношений в сфере информационной безопасности составляет достаточно большое количество директив, конвенций, деклараций, хартий, резолюций, рекомендаций и иных международных актов. Среди них необходимо выделить такие, как Резолюция 54/49 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», принятая 1 декабря 1999 года на 54-й сессии Генеральной Ассамблеи ООН; Конвенция Совета Европы о киберпреступности от 23.11.2001 г.; Конвенция ООН об использовании электронных сообщений в международных договорах 2005 г.; Декларация «О европейской политике в области новых информационных технологий» 1999 г. ; Декларация принципов построения информационного общества, принятая на Всемирной встрече на высшем уровне в Женеве в декабре 2003 г.; Рамочное решение Европейского Союза об атаках на информационные системы от 24.02.2005 г.; Рекомендация Совета Европы по защите неприкосновенности частной жизни в Интернете от 23.02.1999 г.; Рекомендация Совета Европы № Rec (2001) 3 по предоставлению судебных и других правовых услуг гражданам с помощью новых технологий от 28.02.2001 г.; Рекомендация Совета Европы № 1706 «Средства массовой информации и терроризм» 2005 г.; Тунисское обязательство, принятое на Всемирной встрече на высшем уровне по вопросам информационного общества в 2005 г. и др.

Среди методов обеспечения информационной безопасности системообразующими являются методы нормативного правового регулирования общественных отношений в информационной сфере. При этом в силу глобализации информационного общества весьма существенным является международно-правовой режим информационной безопасности. Такой режим создается нормами международного права, в том числе нормами *международного гуманитарного*

права, которое устанавливает правила ведения военных конфликтов, включая нормы регулирования отношений *в информационной сфере*. Эти нормы в равной степени должны распространяться и на *информационные войны* (операции). Концепция международного гуманитарного права основана на триаде *«гуманность — боевая необходимость — соразмерность».* Важнейшими международными актами новейшей истории являются Окинавская хартия глобального информационного общества, Декларация о европейской политике в области новых информационных технологий, Декларация Комитета Министров Совета Европы о правах человека и верховенстве права в информационном обществе и др. Каждый из таких актов предусматривает меры по обеспечению информационной безопасности. Рекомендуется поощрять установление международных *стандартов* и гарантий, необходимых для обеспечения подлинности передаваемых электронными средствами документов и сообщений, имеющих обязательную юридическую силу. Наряду с этим принят также ряд нормативных актов в области *стандартизации*. К их числу можно отнести такие, как Устав международного союза электросвязи от 22.12.1999 г.; Рекомендации Европейской экономической комиссии ООН относительно политики в области стандартизации (1996); Рекомендация № 25 Европейской экономической комиссии ООН «Использование стандарта Организации Объединенных Наций для электронного обмена данными в управлении, торговле и на транспорте» от 09.1996 г.; Рекомендация № 26 Европейской экономической комиссии ООН «Коммерческое использование соглашений об обмене для электронного обмена данными» от 03.1995 г.; Директива Совета Европейского Сообщества № 89/336 «О согласовании законодательных актов государств-участников Сообщества, касающихся электромагнитной совместимости» от 03.05.1989 г.; Рекомендация № R (2003) 15 Комитета министров Совета Европы «Об архивации электронных документов в правовой сфере» от 09.09.2003 г. и др.

Среди нормативных правовых актов государств-участников СНГ необходимо отметить Решение Совета глав правительств СНГ «О концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере» от 04.06.1999 г.; Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств-участников Содружества Независимых Государств в сфере информатизации от 24.12.1999 г.; Соглашение об основах гармонизации технических регламентов государств-членов Евразийского экономического сообщества от 24.03.2005 г. и др.

На международном уровне первая попытка комплексного рассмотрения проблем компьютерной безопасности в уголовном праве была предпринята Организацией экономического сотрудничества и развития (ОЭСР) в 1986 году, затем аналогичные попытки предпринимались в 1989 г. Комитетом Министров стран-членов Совета Европы, в 1996 г. был принят Модельный уголовный кодекс для стран-участниц СНГ, а 23.11.2001 г. была принята Конвенция Совета Европы о киберпреступности, которая упорядочила составы компьютерных преступлений. Однако трансграничный характер таких преступлений, трудности их локализации и доказывания в судах стимулировали развитие практики комплексного обеспечения информационной безопасности на основе ведомственных, отраслевых, национальных и международных стандартов, которые стали динамично разрабатываться и повсеместно использоваться. Это привело к созданию Международной Электротехнической Комиссии (МЭК), а затем и Международной Организации по Стандартизации (ИСО) (см.: http://www.isaudit.ru/itvalue.html). Стандарты часто еще называют лучшими практиками. Их количество увеличивается в связи с растущим многообразием обстоятельств, в которых они применяются как стандарты de facto. Стандарты образуют иерархическую систему. По состоянию на апрель 2007 г. такая система насчитывает несколько десятков стандартов, применение которых комплексно обеспечивает безопасность и качество функционирования человеко-машинных систем на всех этапах их жизненного цикла. Высокоуровневые стандарты часто называют процессными, процедурными или тактическими, так как они описывают процессы, процедуры. К их числу относятся такие, как:

- Управление информационными системами — COBIT, BS 15000, Microsoft Operations Framework и ITIL;
- Управление проектами — PRINCE2 и PMBOK;
- Управление безопасностью — ИСО 13335, ИСО 13569 (банковские и финансовые услуги), ИСО 17799/BS 7799-2 (оба локализованы для многих стран), IT Baseline Protection Manual (Германия), ACSI-33 (Австралия), множество стандартов Национального инсти-

тута стандартов и технологий США (НИСТ/NIST) — *NIST Handbook* (SP800-12, USA), CobiT® *Security Baseline*™, ENV12924 (Медицинская информатика) и Information Security Forum *Standard of Good Practice*[1];

- □ Управление качеством — ИСО 9001, EFQM и Baldrige National Q-Plan;
- □ Программирование — TickIT, Capability Maturity Model Integration (Институт технологий разработки программного обеспечения, SEI);
- □ IT Governance — COBIT, *IT Governance Implementation Guide*, COSO *Internal Control — Integrated Framework* и COSO *Enterprise Risk Management — Integrated Framework*, а также недавно разработанный Австралийский стандарт AS 8015-2005 (корпоративное управление информационными и коммуникационными технологиями);
- □ Управление рисками — Австралийский стандарт AS/NZS 4360[2];
- □ BCP (планирование непрерывности бизнеса) — PAS-56 Британского института стандартов и Австралийский стандарт HB 221-2004;
- □ Аудит ИС — COBIT и ИСО 19011;
- □ Наибольшее и универсальное распространение из процессных стандартов получили стандарты ИСО 17799, COBIT, ИСО 9001, BS 7799-2 и их сочетания.

Кроме большого числа процессных стандартов, имеется еще большее число эксплуатационных, технических стандартов. Международная организация по стандартизации (ИСО), Европейский институт по стандартизации в области телекоммуникаций и Национальный институт стандартов и технологий США (НИСТ/NIST) издали стандарты по таким вопросам, как шифрование (FIPS 197), критерии (технические) оценки безопасности ИТ (ИСО 15408), планирование непрерывности бизнеса (FIPS 87), использование паролей (FIPS 112) и др. Стандарты информационной безопасности, качества и управления в обязательном порядке учитываются при проведении сертификации и аудита. Использование стандартов увеличивает ценность продуктов, создаваемых информационными технологиями, но нет таких стандартов, которые охватывали бы все аспекты управления информационной безопасностью. Состояние вопроса в этой области аналогично состоянию вопроса в системном анализе, ибо последний вырабатывает плохие решения по сложным проблемам, по которым другими методами вырабатываются еще худшие решения.

Начало нынешнего века на уровне Международной организации по стандартизации (ИСО) ознаменовалось тем, что подкомитет «Программная инженерия» был преобразован в подкомитет «Системная и программная инженерия» (SC7 JTC1), что отражает стремление к целостному решению проблем стандартизации информационных технологий в направлении всеобъемлющего качества именно используемых систем в их жизненном цикле (а не составных компонентов или процессов).

Сложившаяся на начало 21-го века структурная организация разработки международных стандартов в области системной и программной инженерии и участие в ней России отражены на рис 2.

Национальные органы по стандартизации платят ежегодные членские взносы, из которых финансируется деятельность международных секретариатов до уровня подкомитетов включительно. По заявкам национальных органов подкомитеты разрабатывают согласованные планы выпуска стандартов.

Каждый международный стандарт разрабатывается в среднем 3-5 лет. Проекты разрабатываются и обсуждаются коллегиально в рабочих группах (при этом учитываются тысячи замечаний), после чего рассылаются на согласование в национальные органы. Деятельность участников рабочих групп ведется на английском языке без перевода и финансируется, как правило, национальными промышленными компаниями, заинтересованными в создании соответствующих стандартов. Стандарт считается принятым, если за него положительно проголосовали более 75% членов Международной организации по стандартизации (ИСО).

Центральное место в ИСО и Международной электротехнической комиссии (МЭК) занимает 7-й подкомитет объединенного технического комитета «Информационные технологии» (SC7 JTC1 ИСО/МЭК). Секретариат располагается в Канаде. Область деятельности подкомитета охватывает стандартизацию процессов, обеспечивающих средств и технологий для проектирования программных продуктов и систем, созданных человеком. Стандарты увязывают различные дисциплин,

---

[1] Совет Европы и Россия. Сборник документов / Отв. ред. Ю.Ю. Берестнев. — М.: Юрид. лит., 2004. — 928 с. — С. 860.

[2] Australian Communications-Electronic Security Instruction 33, www.dsd.gov.au/infosec/publications/acsi33.html.

Рис. 2 Структурная схема организации разработки международных стандартов в области системной и программной инженерии

такие, как промышленная инженерия, менеджмент качества, безопасность, надежность, информационные технологии, управление проектами.

Подкомитет SC7 «Системная и программная инженерия» включает в свой состав системные рабочие группы SWG1 («Группа планирования») и SWG5 («Группа управления архитектурой») и рабочие группы по направлениям: WG2 «Документация», WG4 «Средства и среда», WG6 «Измерение и оценка программного продукта», WG7 «Управление жизненным циклом», WG9 «Системные гарантии», WG10 «Оценка процесса», WG12 «Измерение функционального размера», WG19 «Языки моделирования», WG20 «Орган знаний в программной инженерии», WG21 «Управление активами», WG22 «Терминология».

Стратегическими направлениями подкомитета до 2008 г. выбраны:

- системная интеграция с ориентацией на разработку общесистемных стандартов во взаимодействии с техническими комитетами по качеству (ТС176), надежности (ТС56), функциональной безопасности (SC65A), информационной безопасности (SC27) и др.;
- ключевое партнерство с международными организациями в области стандартизации — Институтом инженеров по электронике и электротехнике, отделением компьютерных наук (IEEE-CS), Международным Советом по системной инженерии (INCOSE) и др.;
- активная связь с рынком и расширение на рынке ниши системной инженерии.

К апрелю 2004 г. всего за время существования SC7 с 1997 г. было создано 79 стандартов. Основными достижениями являются стандарты ИСО/МЭК 15288-2002 «Системная инженерия — Процессы жизненного цикла систем», ИСО/МЭК 12207-95 «Программная инженерия — Процессы жизненного цикла программных средств», ИСО/МЭК 9126-2000 «Информационная технология — Качество программного продукта», ИСО/МЭК 14598 «Информационная технология — Оценка программных продуктов», ИСО/МЭК 15504 «Информационная технология. Оценка процессов, осуществляемых с программными средствами». В 2003-2004 гг. подкомитетом «Системная и программная инженерия» были опубликованы стандарты и технические отчеты (ТО):

- ИСО/МЭК ТО 9126-2: «Программная инженерия — Качество программного продукта — Часть 2: Внутренние показатели»;
- ИСО/МЭК ТО 9126-3: «Программная инженерия — Качество программного продукта — Часть 3: Внешние показатели»;
- ИСО/МЭК ТО 14143-3:2003 «Информационная технология — Измерение программных средств — Измерение функционального размера — Часть 3: Верификация методов измерения функционального размера»;
- ИСО/МЭК ТО 19500-2:2003 «Информационная технология — Открытая распределенная обработка — Часть 2: Общий ORB-протокол взаимодействия (GIOP)/ Интернет ORB-протокол взаимодействия (IIOP)»;
- ИСО/МЭК ТО 19760 «Системная инженерия — Руководство для ИСО/МЭК 15288 (Процессы жизненного цикла системы)»;
- ИСО/МЭК ТО 19761 «Программная инженерия — COSMIC-FFP — Метод измерения функционального размера»;
- ИСО/МЭК ТО 20926 «Программная инженерия — IFPUG 4.1 Опытный метод измерения функционального размера — Практическое руководство для расчетов»;
- ИСО/МЭК ТО 9126-4 «Программная инженерия — Качество программного продукта — Часть 4: Показатели потребительского качества (при использовании)»;
- ИСО/МЭК ТО 14143-5 «Информационная технология — Измерение программных средств — Определение измерения функционального размера — Часть 5: Определение функциональной области для использования функционального размера»;
- ИСО 90003 «Руководство для применения ИСО 9001:2000 для программных средств»;
- ИСО/МЭК 15504-3 «Программная инженерия — Оценка процесса — Часть 3: Выполнение оценки»;
- ИСО/МЭК 18019 «Системная и программная инженерия — Руководство для проектирования и подготовки пользовательской документации для применения программных средств».
- Проекты, находящиеся по состоянию на 2004 г. в разработке и ожидании окончательного решения:
- FDIS 15476 «Программная инженерия — CDIF Семантическая метамодель — части 3, 4, 5»;
- FDIS 15909 «Программная инженерия — Сети Петри высокого уровня — Часть 1: Концепции, Определения и графические обозначения»;
- DIS 19501-1 «Унифицированный язык моделирования UML PAS»;
- DTR 19759 «Руководство для органов знаний в области программной инженерии» (SWEBOK);
- DIS 24570 «Программная инженерия — Руководства по определениям и расчетам для применения анализа функционального смысла»;
- ИСО/МЭК FCD 9127 «Программная инженерия — Пользовательская документация и информация для пакетов программ потребителя»;
- ИСО/МЭК DTR 9249 «Информационная технология — Руководство для управления программной документацией»;
- ИСО/МЭК FDIS 15504-4 «Программная инженерия — Оценка процесса — Часть 4: Руководство по использованию процесса усовершенствования и процесса определения возможности»;
- ИСО/МЭК FCD 15940: «Информационная технология — Программная инженерия — Сервисы среды»;
- «Системная и программная инженерия» — Словарь;
- проект по гармонизации ИСО/МЭК 15288 и 12207;
- ТО 14143-6 «Информационная технология — Измерение программных средств — Определение измерения функционального размера — Часть 6: Руководство для использования серии стандартов ИСО/МЭК 14143 и связанных с ними международных стандартов»;
- ИСО/МЭК 16085 «Программная инженерия — Процессы жизненного цикла программных средств — Управление рисками»;
- ревизия стандартов серии «Программная инженерия — Процессы жизненного цикла программных средств — Сопровождение ИСО/МЭК 14764»;
- ревизия ТО 14471-99: «Программная инженерия — Руководство для усвоения CASE-средств»;
- ревизия стандарта IS 14102-95 «Информационная технология — Руководство для оценки и выбора CASE-средств».

Новыми рассматриваемыми проектами, планируемыми подкомитетом «Системная и программная инженерия» на ближайшую перспективу, являются:

- перенос стандарта МЭК/ТС 56 (проект 61720): «Руководство по методикам и средствам для достижения доверия к программному обеспечению»;

- ревизия и отслеживание стандарта IEEE 1220 «Стандарт IEEE по применению и управлению процессом в программной инженерии»;
- ревизия и отслеживание стандарта EIA 632 «Стандарт Альянса отраслей электронной промышленности США — Процессы для проектирования систем»;
- ревизия стандарта ИСО/МЭК 14102 «Информационная технология — Руководство для оценки и выбора CASE-средств»;
- ревизия стандарта ИСО/МЭК ТО 14143-1:1998;
- сопровождение проекта по использованию ITU-T Rec/X/901-3 ИСО/МЭК 10746 Части 1-3 «Эталонная модель для открытой распределенной обработки»;
- отслеживание стандарта IEEE 2001 «Рекомендованная IEEE практика для Интернета — Инженерия, управление и жизненный цикл сайтов»;
- отслеживание стандарта ANSI NCITS 354-2001 «Американский национальный стандарт для информационных технологий — Общий промышленный формат для отчетов по испытаниям применимости».

Наибольший интерес представляет международная практика регулирования ин- формационных отношений и угроз, связанных с использованием глобальной сети Интернет. К основным элементам информационного правоотношения относятся: субъекты, вступающие в правоотношения при осуществлении информационных процессов; объекты, в связи с которыми субъекты вступают в информационные правоотношения, содержание прав и обязанностей субъектов по осуществлению действий над объектами информационного правоотношения, ответственность субъектов при нарушении прав или невыполнении обязанностей по отношению к другим субъектам правоотношения. Субъектами информационных правоотношений являются оператор Интернет-связи, его абонент, другие пользователи Интернет, правоохранительные органы. Содержание прав и обязанностей перечисленных субъектов взаимосвязано с их возможностями совершать определенные действия с объектами информационных правоотношений, в том числе и причиняющие вред. Объектами в информационных отношениях абонента и оператора Интернет-связи являются информация, информационные продукты и услуги, состояние защищенности личности, защищенность информации. Действия субъектов таких отношений, способных повлиять на информационную безопасность личности, являются основанием их ответственности. К возможным действиям абонента относятся: просмотр веб-страниц, получение и отправка электронных сообщений, хостинг. К возможным действиям оператора Интернет-связи относятся сбор сведений об информационном обмене абонента, воздействие на информационный обмен абонента путем изменения скорости обмена, фильтрации содержимого передаваемой информации, воздействия на информацию, опубликованную пользователем на веб-странице, размещенной на сервере оператора, сбор персональных данных о пользователе. Возможные действия правоохранительных органов заключаются в истребовании от оператора Интернет-связи или его абонента необходимой им информации об информационном обмене абонента. К действиям других пользователей Интернета, имеющих значение для информационной безопасности абонента, можно отнести только намеренные действия по получению несанкционированного доступа к его информации на веб-странице, в компьютере, в электронном письме. Просмотр веб-страниц несет в себе две угрозы. Это вредная информация, размещенная непосредственно на странице (фото, видео, аудио, текстовые данные), и вредоносные программные коды, запускаемые с различными приложениями, которые обеспечивают правильное отображение просматриваемой страницы, способные изменить состояние информации в компьютере пользователя. Вредная информация способна оказывать воздействие на пользователя при посещении веб-страниц, на которых она расположена. Попадание вредной информации на экран монитора пользователя зависит, в основном, от действий самого пользователя, так как он сам осуществляет передвижение по сети Интернет, и решает, какая информация подлежит его вниманию. Ограничение на доступ к вредной информации может быть установлено самим оператором Интернет-связи. Это возможно за счет применения им специальных программных фильтров, позволяющих перекрывать доступ к информации определенного содержания, в том числе и не относящейся к вредной. Большинство операторов Интернет-связи имеют программные фильтры и могут применять их по договоренности с абонентом. Другим видом действий абонента является получение электронных сообщений. В этом случае существуют угрозы воздействия вредной информации, размещенной в электронном сообщении, получение и заражение компьютерными вирусами, получение не запрашиваемой информации *(спам*)

В действиях пользователя по отправке электронных писем существуют такие угрозы, как недоставка отправленного письма адресату и нарушение конфиденциальности информации, содержащейся в письме. Данные угрозы могут быть реализованы как в результате действий самого пользователя, так и в результате действий или бездействия оператора Интернет-связи. Так, при отсутствии соединения или при некачественном соединении с сетью Интернет абонент не сможет отправить электронную корреспонденцию. Кроме того, угроза недоставки электронного письма или нарушения его конфиденциальности может быть реализована в результате неправильной работы почтовых серверов оператора Интернет- связи, в результате использования фильтров на исходящую от абонента информацию или в силу форс-мажорных обстоятельств. Нарушение конфиденциальности электронной переписки абонента может произойти в результате несанкционированного доступа третьих лиц к его компьютеру или электронному почтовому ящику. При опубликовании своей веб-страницы в сети Интернет для информационной безопасности пользователя существуют такие угрозы, как несанкционированный доступ к опубликованной информации и, следовательно, нарушение данных аутентификации абонента, изменение или удаление веб-страницы пользователя и ее блокировка как результат несанкционированного доступа. Источником таких угроз может быть как оператор Интернет-связи, так и другие пользователи Интернет. В первом случае возможность несанкционированного доступа возможна в силу того, что оператор Интернет-связи является хранителем данных аутентификации (пароля и логина) пользователя при доступе к редактированию своей страницы. Во втором случае доступ к странице абонента может быть осуществлен в силу получения другими пользователями Интернет данных аутентификации, необходимыми для управления страницей. Данная информация может быть получена в результате ее хищения путем несанкционированного доступа к файлам (взлома) оператора Интернет-связи или любым другим способом. Еще существуют угрозы, возникновение которых не зависит от деятельности абонента в глобальной сети. К ним относятся диффамация, нарушение авторских прав, распространение персональных данных.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому вопрос аудита «как оценить уровень безопасности корпоративной информационной системы» обязательно влечет за собой следующие: в соответствии с какими критериями производить оценку эффективности защиты, как оценивать и переоценивать информационные риски предприятия? Вследствие этого, в дополнение к требованиям, рекомендациям и руководящим документам Государственной комиссии по техническому и экспортному контролю (ранее Гостехкомиссии, далее по тексту Гостехкомиссии по тем подзаконным актам, которые были выпущены ею до Административной реформы) России приходится адаптировать к нашим условиям и применять методики международных стандартов (ИСО 17799, 9001, 15408, стандартов Британского института стандартов и пр.), а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности инвестиций в обеспечение безопасности и защиты информации. В зарубежных нормативных документах установлен набор требований для различных типов средств и систем информационных технологий, в зависимости от различных условий их применения. Особенности развития отечественной нормативной базы в данной области заключаются в том, что отсутствует комплексный подход к проблеме защиты информации (рассматриваются в основном вопросы несанкционированного доступа к информации и вопросы обеспечения защиты от побочных электромагнитных излучений и наводок) и, кроме того, разработанные национальные стандарты и руководящие документы Гостехкомиссии России 1992-1996 не принимали во внимание международные стандарты ИСО/МЭК. На сегодняшний день эти недостатки начали устраняться. В целях совершенствования отечественной нормативной базы с 2001 года Гостехкомиссия и Госстандарт России совместно с другими заинтересованными министерствами и ведомствами реализуют новые инициативы в этом направлении. В частности, утверждены три стандарта, определяющие критерии оценки безопасности информационных технологий. Они устанавливают требования к формированию заданий по оценке безопасности в соответствии с положениями международных стандартов. По линии Гостехкомиссии созданы несколько руководящих документов, в том числе «Руководство по разработке профилей защиты», «Руководство по регистрации профилей

защиты», «Методология оценки безопасности информационных технологий» и «Автоматизированный комплекс разработки профилей защиты». Перечисленные документы, по сути, представляют собой прямую трансляцию положений международных стандартов ИСО на российскую нормативно-техническую базу. В дополнение к ним создаются еще шесть спецификаций на защитные профили для операционных систем, межсетевых экранов, систем управления базами данных, автоматизированных систем учета и контроля ядерных материалов и др. Утвержден государственный стандарт РФ, определяющий процессы формирования средств проверки электронной цифровой подписи, идет работа по переводу данного стандарта в категорию межгосударственного. В 2000-2001 гг. была создана «Программа комплексной стандартизации в области защиты информации на 2001-2010 годы» (ПКС), в которой применен комплексный метод стандартизации. ПКС предусматривает появление примерно 40 ГОСТов. Кроме того, ВНИИ «Стандарт» разрабатывает проект «Программы комплексной стандартизации в области защиты информации, составляющей государственную тайну». В ее рамках планируется принятие 42 национальных стандартов и других нормативных документов. В свою очередь, Госстандарт разработал и представил на утверждение в Правительство РФ проект «Программы по разработке технических регламентов на 2003-2010 годы». В ходе ее выполнения создаются следующие документы: «Общий технический регламент безопасности информационных технологий», «Общий технический регламент требований к системам безопасности информационных технологий», «Общий технический регламент требований по защите информации, обрабатываемой на объектах информатизации» и «Специальный технический регламент требований по защите информации в оборонной промышленности». В 2003 году Госстандарт разработал проект классификатора техники и средств защиты информации, требований к контролю над эффективностью средств защиты информации и соответствующих систем управления. Создан проект государственного стандарта, включающего в себя общие положения по формированию системы управления качеством при разработке, изготовлении, внедрении и эксплуатации техники защиты информации. Внедрение этих нормативных документов обеспечит единую классификацию механизмов и техники защиты информации, позволит определить основные характеристики систем качества техники защиты информации. Благодаря этому уменьшится разобщенность разработчиков и изготовителей, повысится уровень координации производителей специальной аппаратуры. Из анализа действующих нормативных документов по стандартизации в данной области следует, что по охвату регулирования аспектов безопасности ИТ, по детализации рассматриваемых в них проблем российские национальные стандарты все еще уступают международным. Вопросы стандартизации в сфере безопасности ИТ решаются на международном уровне — совместным техническим комитетом СТК1 ИСО/МЭК «Информационные технологии», на региональном — европейскими организациями CEN, ECMA и др., на национальном уровне — ANSI, NIST (США), DIN (Германия) и др.

При использовании международного правового регулирования информационной безопасности можно сформулировать следующие проблемы, связанные с его использованием:

- необходимость работать с информацией разного типа (структурированная и неструктурированная);
- разнородность источников и форматов данных (телевидение, радио, печатные издания, Интернет, базы данных и пр.);
- большие объемы данных;
- необходимость гибко и оперативно настраивать систему на различные задачи в соответствии с меняющейся обстановкой;
- необходимость синхронизации мощностей системы с нарастающими потоками данных («масштабируемости»);
- необходимость эффективно анализировать данные в распределенной среде;
- необходимость прогнозирования развития ситуаций, например, по модели «что, если…»;
- необходимость мониторинга открытого информационного пространства (Интернет/СМИ);
- необходимость применять максимально стандартизованные решения.

Решение перечисленных проблем требует применения современных аналитических систем для качественного обеспечения использования международного опыта правового регулирования информационной безопасности [8]. На этой основе представляется возможным создание и использование единого международного правового пространства, которое, по нашему мнению, сделает возможным эффективное использование международного опыта нормативно-правового регулирования процессов обеспе-

чения информационной безопасности в Российской Федерации.

Основные процессы сегодняшнего этапа государственного строительства России в области информационной безопасности требуют от структур, обеспечивающих принятие органами государственной власти обоснованных решений, постоянного совершенствования эффективности работы на следующих направлениях деятельности:

- □ непрерывный мониторинг и взвешенная аналитическая оценка глобальных направлений укрепления безопасности России;
- □ формализация этих направлений в виде частных проблем и формулировка их путей их решения;
- □ интегрированное ситуационное моделирование этих проблем;
- □ выработка ранжированных вариантов (способов и средств) решения сформулированных частных проблем.

Перечисленные направления деятельности характеризуются:

- □ коллективностью — участием в процессе большого количества взаимодействующих физических и юридических лиц;
- □ интеллектуальностью — вследствие объективно нечеткой постановки и слабой формализованности проблемы доля интеллектуальных действий остается значительной;
- □ интерактивностью — частой чередуемостью действий, выполняемых человеком и программно-техническими средствами;
- □ уникальностью — отсутствием типовых полномасштабных технологий реализации обсуждаемых проблем;
- □ важностью визуальной и аудиоинформации, доля которой в общем объеме значительна.

Функционально указанные выше направления деятельности реализуются формированием высококвалифицированных групп экспертов (по перечню проблем) и оснащением их технологиями извлечения и анализа информации, содержащейся в источниках различной природы, а также эффективного контроля состояния защищенности и обеспечения безопасности, в том числе от несанкционированного доступа, добытой и используемой в работе информации.

В настоящее время эффективным инструментом решения проблемы информационного обеспечения групп экспертов являются программно-аппаратные комплексы (ПАК) автоматизированного поиска и обработки информации, а также контроля защищенности собственных информационных ресурсов, разрабатываемые рядом российских компаний, специализирующихся в области создания автоматизированных систем и информационных технологий в интересах противодействия криминальным структурам и терроризму.

Основными задачами, решаемыми программно-аппаратными комплексами, являются:

- □ обеспечение лиц, принимающих решения, актуальной, достоверной и полной информацией, в том числе поиск во внешних и внутрикорпоративных сетях структурированных и неструктурированных данных, получение, подготовка и хранение информации, обеспечивающей принятие оптимальных решений;
- □ упреждающее выявление угроз финансово-экономического, социально-психологического и иного характера как внутри организаций, так и в сфере их интересов;
- □ обнаружение среди анализируемых лиц и организаций субъектов, имеющих признаки связи с вероятными источниками угроз (криминальными и террористическими организациями, лицами, а также структурами, аффилированными с ними, конкурентами, мошенниками, фирмами-банкротами, предъявителями фальшивых документов и др.);
- □ информационная поддержка расследования случаев нанесения ущерба организации, систематизация результатов расследований для последующего использования;
- □ оценка кандидатов при приеме на работу (места прежней работы, репутация кандидата и фирм, где он работал; возможные связи с лицами и организациями, конкурентами, партнерами по рынку, криминальными и мошенническими структурами; причастность к чрезвычайным происшествиям, характер и объекты собственных коммерческих интересов и т. п.);
- □ контроль и анализ состояния защищенности информационных ресурсов, конфиденциальных сведений организаций, а также внутренних и внешних коммуникационных сетей организации (Интранет и Интернет), в том числе:
  - комплексный анализ трафика глобальных и локальных сетей передачи данных, включающий прием и декодирование протоколов, выделение из трафика данных (сообщений) и регистрация их, контент-анализ в реальном масштабе времени или в отложенном режиме;

- возможность как анализа сетевого трафика, так и реконструкции сессий, выделения сообщений и проведения анализа контента (содержимого), передаваемого в локальных сетях;
- широкий спектр поддерживаемых протоколов для всех семи уровней модели OSI и обеспечение одновременной работы по нескольким каналам.

В последнее время бурно развиваются информационные технологии, что сопровождается стремительным увеличением объемов передаваемой информации; это значительно усложняет ее непосредственную обработку. Меняются характер и формы представления информации. Большая часть информации является неструктурированной и содержится в динамических потоках и файлах разнообразных форматов: текстовых, мультимедийных и пр. Значительная часть информации является па- разитной (реклама, спам), дублируется полно- стью или частично.

Необходимость охвата и обобщения огромных динамических разнородных информационных потоков, а также непредсказуемость характера представляющих интерес данных приводит к постепенному отказу от использования в качестве единственного критерия отбора наличия в них определенных слов и развитию новых подходов к их обработке. Все большее применение получают интеллектуальные технологии работы с информацией. Основанные на таких технологиях новые методы обработки данных направлены на более эффективное выявление необходимой информации из огромных объемов, с одной стороны, и ее комплексный анализ для извлечения скрытых, ранее неизвестных знаний — с другой. В результате внедрения таких технологий значительно повышается эффективность и оперативность обработки информации, снижаются объемы ресурсов и влияние человеческого фактора.

Информационно-аналитическая система (ИАС) предназначена для отбора информации из разнородных источников, ее автоматической аналитической обработки, извлечения знаний с целью раннего выявления угроз безопасности и поиска путей их нейтрализации, оповещения о появлении искомой информации в режиме, близком к режиму реального времени, углубленного анализа, составления и представления аналитических отчетов и прогнозов развития ситуации. Другими словами, ИАС позволяет осуществлять круглосуточный мониторинг информационного пространства.

Принципиальной особенностью, отличающей ИАС от существующих на рынке систем, является, во-первых, способность системы обрабатывать как текстовую, так и мультимедийную информацию (аудио- и видеопотоки и записи) и, во-вторых, поддержка полного цикла обработки данных, то есть преобразование данных в информацию, извлечение знаний из информации путем фактографического и контент-анализа, концептуальное моделирование.

В качестве источников данных для ИАС могут выступать любые известные источники информации (интернет, файловые системы, базы данных, аудио- и видеоканалы). ИАС способна работать как с потоком, так и с файлами практически всех известных форматов. Обобщенная схема функционирования ИАС приведена на рис. 3.

- □ Основу ИАС составляют следующие модули (инструменты):
- □ Модуль анализа и визуализации результатов;
- □ Модуль моделирования ситуаций и прогнозирования;
- □ Модуль поиска и анализа информации;
- □ Модуль обработки структурированных данных;
- □ Хранилище данных.

Взаимодействие модулей показано на рис.4.

Модуль поиска и анализа информации предназначен для решения задач сбора данных из различных источников (Интернет, СМИ, телевидение, радио, базы данных); создания единого индекса по всем источникам; извлечения информационных объектов и связей для автоматизации процессов анализа; классификации, категоризации и кластеризации; обеспечения различных видов поиска, поддержки справочной информации по объектам.

Модуль обработки структурированных данных реализует набор методик и математических алгоритмов, позволяющих рассчитывать комплексные и интегрированные показатели на основе структурированной части результатов социологических опросов населения, показателей социально-политической ситуации и социально-экономического развития регионов.

Модуль анализа и визуализации результатов поддерживает виды анализа, позволяющие полноценно оценивать ситуации: многомерный, выборочный, непоследовательный, анализ временных рядов и анализ рынков. Ключевыми функциями модуля являются организация единой аналитической среды для поль-

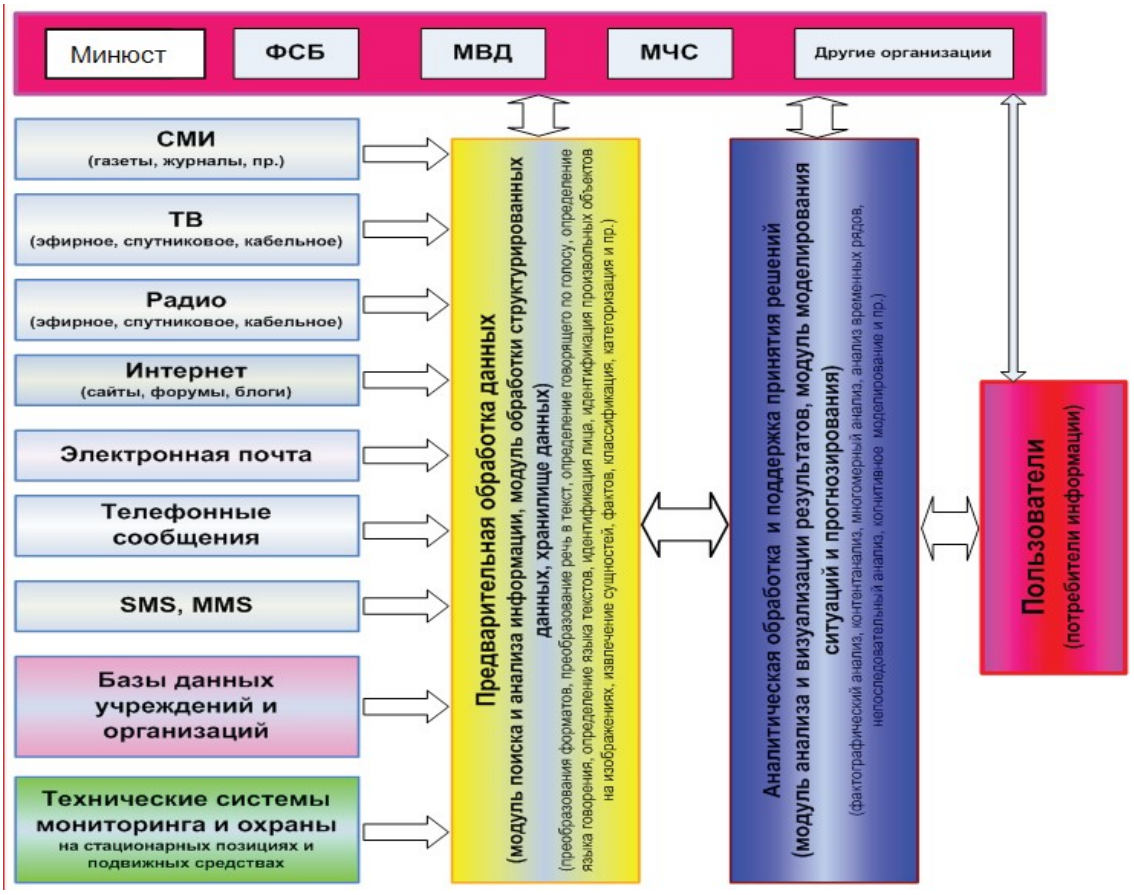

Рис.3. Схема функционирования ИАС

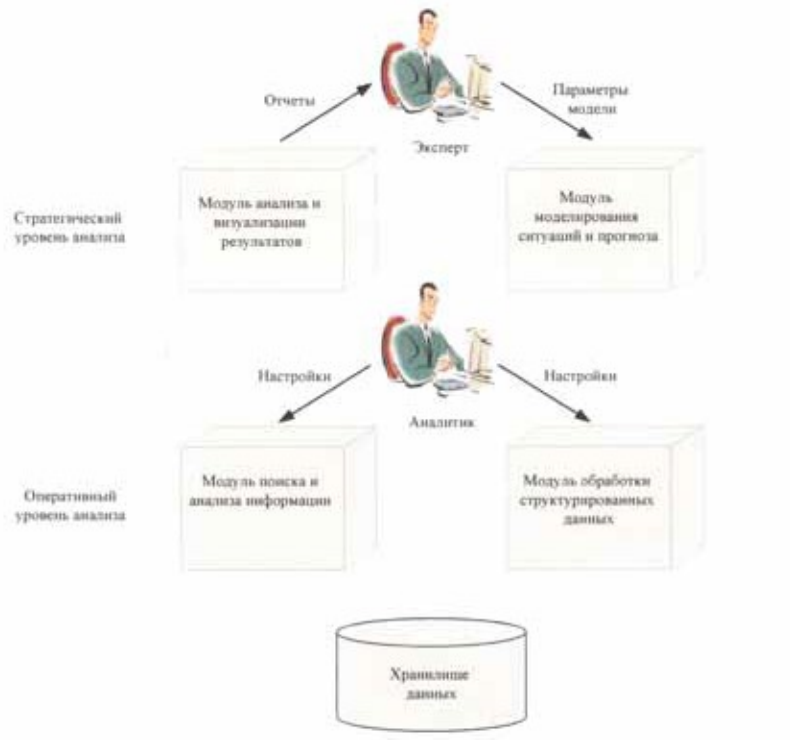

Рис. 4 Взаимодействие аналитиков и специалистов с модулями системы

зователей; реализация аналитической функциональности и визуализация; интеграция в единой системе отчетности данных из различных источников; создание аналитической платформы для стратегического развития путем формирования фундаментальной информационной модели.

Основными функциями модуля моделирования ситуаций и прогнозирования являются организация аналитической среды, сценарное моделирование развития ситуаций и поддержка принятия решений о выборе эффективных способов достижения целей развития ситуации.

Хранилище данных предназначено для создания единого информационного пространства, позволяющего сформировать масштабируемую платформу для анализа информации в гетерогенной среде. Оно позволяет интегрировать различные функциональные модули системы, объединяя их через базу данных. Сбор данных из существующих источников осуществляется модулем поиска и анализа информации.

Информационно-аналитическая система построена по модульному принципу, т. е. возможен выбор любой комбинации модулей и языков для решения конкретных задач. ИАС построена по технологии «тонкого клиента», т. е. как сама система, так и ее пользователи могут быть пространственно разнесены. При этом от пользователей системы не требуется установки какого-либо специального программного обеспечения.

ИАС в своем функционировании реализует следующие технологии:

- интеллектуальный поиск, индексация, классификация и категоризация;
- фонемный поиск;
- идентификация говорящего по голосу;
- распознавание образов;
- идентификация лиц;
- распознавание текста и бегущей строки;
- преобразование речи в текст;
- анализ и визуализация результатов;
- концептуальное моделирование.

Каждый входящий файл (сообщение, документ) подвергается предварительной обработке. Документы (файлы форматов doc, pdf, html и др.) анализируются на предмет содержания в них графических объектов. В случае наличия таких объектов они выделяются в отдельные файлы. Речь, содержащаяся в аудиофайлах и звуковых дорожках видеофайлов, преобразовывается в текст, и определяется принадлежность голоса говорящего (диктора). Видеофайлы анализируются на предмет наличия в них бегущей строки. Если бегущая строка найдена, она преобразуется в текст. В графических файлах, извлеченных из текста, а также кадрах видеофайлов производится поиск и распознавание печатного текста и образов (логотипов, силуэтов и т. п.) и идентификация лиц. Такая информация, содержащаяся в файлах в неявном виде (метаинформация), так же как и текстовое содержание документов, индексируется и становится доступной для поиска и мониторинга.

Основные методы, используемые в работе программно-аппаратного комплекса:

- динамическая категоризация и классификация, аннотирование и аналитическая обработка текстовой и другой неструктурированной информации.
- регистрация, ввод, отбор, хранение и обработка аналогового и цифрового видео, текстов субтитров, временных кодов и метаданных;
- текстовый и визуальный поиск, поиск и распознавание лиц и иных биометрических данных, автоматическая категоризация и классификация текстовой, графической и другой неструктурированной информации, а также распознавание речи;
- фонетический поиск и профилирование аудио- и видеофайлов на основе звуковых образов в человеческой речи;
- многоканальный режим работы; семиуровневое декодирование;
- поддержка более 600 протоколов; экспертная система и автоматическое распознавание протоколов;
- анализ, декодирование и обработка сетевых потоков в реальном масштабе времени;
- анализ взаимодействия сетевых объектов и анализ инкапсулированных протоколов;
- выделение сообщений с формированием файлов из каналов передачи данных с возможностью записи их на диск и последующий контент-анализ их; сбор статистики в режиме онлайн, с записью результатов на диск для последующего анализа;
- LAN интерфейсы: Ethernet 10/100/1000 Мбит/с; WAN интерфейсы: G.703;
- портативность;
- мощный встроенный макроязык, позволяющий писать сценарии работы анализатора в зависимости от изменяющихся характеристик трафика; комплект средств разработки (SDK) для создания собственных декодеров протоколов;

Основными преимуществами ПАК, предложенного в статье [7], являются:

- расширенные поисковые возможности (логический, нечеткий и смысловой поиск), в том числе с использованием естественного языка запросов;
- масштабируемость ПАК по объему архивов;
- гибкость ПАК, в том числе относительно аппаратно-программной платформы;

- ☐ эффективная реализация механизма «горячего развертывания» — доступность архивов во время обновления информации;
- ☐ поддержка большого, по сравнению с другими ПАК, количества форматов данных — около 250, а также реализованная возможность подключения к системе собственных конверторов данных;
- ☐ поддержка широкого круга источников информации (файловые системы, сайты Интернета, базы данных, почтовые системы, специализированные системы управления документами и т. п.);
- ☐ реализованная многоуровневая защита информации;
- ☐ обеспечение контроля доступа на уровне отдельных документов, возможность передачи данных в зашифрованном виде, что обеспечивает гибкое управление правами пользователя;
- ☐ универсальное решение для анализа LAN, WAN сетей; отдельные и комбинированные конфигурации;
- ☐ применение гибкой системы фильтров для разнообразных применений;
- ☐ возможность модернизации программного и аппаратного обеспечения; функциональная гибкость; модульная структура программного и аппаратного обеспечения;
- ☐ оптимальное соотношение: «цена/функциональность».

Представленная в статье информация свидетельствует об актуальности использования международного опыта правового регулирования информационной безопасности для Российской Федерации. Эффективное его использование требует реального создания единого международного нормативно-правового пространства. Создание такого пространства невозможно без использования мощных информационно-аналитических платформ. Таким образом, предлагаемые компанией программно-аппаратные комплексы автоматизированного поиска и обработки информации, а также контроля защищенности собственных информационных ресурсов являются эффективными инструментами информационно-аналитической поддержки государственных структур, обеспечивающих информационную безопасность России.

Литература:

1. Крылов Г.О. Международные проблемы информационного права: учеб. пособие, М.: РПА Минюста России, 2013. — 122 с. — ISBN 978-5-89172-465-5/.
2. Полякова Т.А. Информационная безопасность в условиях построения информационного общества. М.: РПА Минюста России, 2007.
3. Андреев О.О. и др. Под редакцией Васенина В. А. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. М:. МЦМНО, 2008.
4. Андреев О.О. и др. Под редакцией Васенина В. А. Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. М:. МЦМНО, 2008.
5. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М., изд. «Вооружение, политика, конверсия», 2004, 395 с. — www.mathmodels.net
6. Костогрызов А. И., Лазарев В.М., Нистратов Г.А. Математические модели для эффективного контроля и управления качеством компьютеризированных систем в контексте требований системообразующих стандартов. Сборник СФ ФС РФ «Научные основы национальной безопасности», 2005 г.
7. Лазарев В.М., Любимов А.Е. Предложения по использованию информационно-аналитических систем в информационно-правовом обеспечении органов законодательной и исполнительной власти федерального, регионального и местного уровней, статья в сборнике НЦПИ «Правовая информатика», вып. № 1, 2013.
8. Стрельцов А.А. Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации. // Сборник и методологические проблемы информационной безопасности под редакцией В.П. Шерстюка. — МГУ, 2004.