Институт проблем информационной
безопасности МГУ

Научные и методологические проблемы информационной безопасности

(сборник статей)

Под редакцией В. П. Шерстюка

Москва
Издательство МЦНМО
2004

УДК 002
ББК 73
Н34

Н34 **Научные** и методологические проблемы информационной безопасности (сборник статей). Под ред. В. П. Шерстюка. — М.: МЦНМО, 2004. — 208 с.

ISBN 5-94057-147-6

В настоящем сборнике объединены статьи ведущих российских ученых, занимающихся как теоретическими проблемами обеспечения информационной безопасности, так и их практической реализацией. Сборник может быть полезен научным работникам, аспирантам, преподавателям, а также всем, кто интересуется проблемами информационной безопасности и ее обеспечения.

ББК 73

Оглавление

Предисловие

Выход в свет настоящего сборника приурочен к 65-летию ректора Московского государственного университета им. М. В. Ломоносова академика РАН В. А. Садовничего. В современное, весьма непростое для отечественной науки время, на него возложена нелегкая и ответственная миссия организации научных исследований и подготовки кадров в Московском университете, с которым его судьба связана не одно десятилетие, и где он прошел путь от студента до ректора.

Одним из новых направлений научных исследований, поддержанных В. А. Садовничим, является разработка проблем обеспечения информационной безопасности, что обусловлено, в частности, возрастающей ролью информационных технологий в период становления глобального информационного общества.

Важное значение для успешного развития этого направления имеет работа межведомственного междисциплинарного семинара по научным проблемам информационной безопасности, созданного по инициативе и под руководством В. А. Садовничего. Семинар уже более трех лет работает в МГУ, и за это время превратился в авторитетный научный форум. В его заседаниях обычно участвует до 100 ученых различной квалификации — от профессоров до аспирантов, представляющих различные вузы, научные институты и ведомства. В последнее время наблюдается позитивная тенденция в развитии семинара — он становится международным, в его работе стали принимать участие ученые из других стран — как ближнего, так и дальнего зарубежья.

В рамках семинара, при большой активности участников, уже проведено 17 заседаний по наиболее актуальным аспектам технологических и гуманитарных проблем информационной безопасности. В ходе этой работы сформировался круг ученых и специалистов, заинтересованных в развитии проблематики информационной безопасности. Большое число встреч и дискуссий специалистов позволило выработать целый ряд плодотворных научных и организационных предложений, которые реализуются как внутри МГУ, так и в других ведомствах, включая аппарат Совета Безопасности Российской Федерации.

Новый импульс развитию этого направления научных исследований в рамках Московского университета придало создание, при содействии В. А. Садовничего, Института проблем информационной безопасности на базе кафедры информационной безопасности. Деятельность нового института направлена на проведение фундаментальных и прикладных научных исследований проблем безопасности информационного общества, имеющих комплексный междисциплинарный характер, координацию исследований по проблемам безопасности информационного общества, которые ведутся учеными и творческими коллективами МГУ, а также организацию таких исследований в рамках межведомственного междисциплинарного семинара по информационной безопасности.

В настоящем сборнике объединены статьи ряда российских ученых, занимающихся как теоретическими проблемами обеспечения информационной безопасности, так и его практической реализацией. Являясь в определенном смысле выражением результатов работы методологического семинара, эти работы отражают состояние исследований в этой области знания. Они могут быть полезны научным работникам, аспирантам, преподавателям, а также всем, кто интересуется проблемами информационной безопасности и ее обеспечения.

Директор Института проблем
информационной безопасности
МГУ им. М. В. Ломоносова,
член-корреспондент
Академии криптографии
Российской Федерации В. П. Шерстюк

Математические проблемы безопасности информационных технологий

В. А. Садовничий, В. А. Носов, В. В. Ященко

Современные компьютеры, глобальные информационные сети и сетевые технологии сильно изменили нашу жизнь, но вместе с новыми возможностями у нас появились и новые риски. «Как пользоваться такими возможностями, но при этом нейтрализовать риски или хотя бы снизить возможный ущерб от их реализации?» — вот главный вопрос обеспечения безопасности информационных технологий. Для ответа на этот вопрос необходимо решить большое количество разнообразных задач: и политических, и экономических, и научных, и технических.

В нашей статье будут затронуты не только конкретные математические проблемы информационной безопасности, но и некоторые организационно-научные вопросы, связанные с этими проблемами.

Наиболее действенным инструментом обеспечения безопасности информационных технологий является криптография. Год назад на конференции «Московский университет и развитие криптографии в России» состоялся подробный разговор о развитии криптографии, как науки, в XX веке и о влиянии криптографии на развитие математики. Хотелось бы продолжить этот разговор и подчеркнуть несколько особенностей развития криптографии в последние годы.

Во-первых, под влиянием процессов глобальной информатизации резко расширился круг заказчиков и потребителей криптографической продукции. Поэтому в криптографии происходит «размежевание» идей, методов и результатов, предназначенных для защиты государственных секретов, и, так сказать, «для массового потребления». Конечно же, такое размежевание необходимо и естественно, поскольку у заказчиков принципиально

разные могут быть требования как по уровню защиты информации, так и по стоимости защиты.

Во-вторых, постоянно растет количество публикаций по криптографии (и научных, и псевдонаучных). Это происходит не только из-за расширения круга заказчиков, но также и вследствие стремительного роста числа приложений криптографии и новых научных задач, инициированных криптографией. Поскольку раньше базовые криптографические знания были секретными, то даже вполне квалифицированные ученые, подключаясь к решению таких новых задач, допускают вполне объяснимые криптографические ошибки. Следовательно, нужна открытая (в допустимых пределах) криптографическая литература — и фундаментальные монографии, и учебники, и научно-популярная литература. Следует отметить, что за последние 5 лет в стране уже вышло несколько серьезных книг по криптографии, но этого явно недостаточно.

В-третьих, активно развивается международное научное сотрудничество по проблемам информационной безопасности. Так, Московский университет уже 3 года сотрудничает с Консорциумом военных академий и институтов, изучающих проблемы безопасности. В 2001 году в МГУ прошла конференция по информационной безопасности, в которой приняло участие более 500 ученых и специалистов из 45 стран. После конференции наши ученые участвовали в нескольких международных мероприятиях по проблемам информационной безопасности и борьбы с кибертерроризмом. Наш опыт международного научного сотрудничества в этой области показал, что иногда мы с зарубежными коллегами говорим на разных языках. Это отчасти объясняется тем, что до сих пор не выработана единая международно-признанная терминология. Например, существуют разные трактовки содержания и соотношения понятий «информационная безопасность», «безопасность информационных технологий», «безопасность информации», «безопасность киберпространства». Московский университет выступил с инициативой разработки многоязычного глоссария по проблемам безопасности информационного общества, и в настоящее время ведутся переговоры о создании международного коллектива для проведения этой работы. Одновременно с этим мы совместно с Академией криптографии Российской Федерации разрабатываем открытый русско-английский и англо-русский словарь криптографических терминов. Это

тяжелая и очень объемная работа, в ней много дискуссионных вопросов, уходящих корнями и в историю, и в секретность. Тем не менее, мы надеемся в следующем году издать такой словарь.

Хотелось бы подчеркнуть одну важную особенность последних лет: наряду с развитием традиционных математических направлений криптографии (алгебраическое, теоретико-числовое, комбинаторное и т. д.) происходит формирование нового направления, которое можно назвать математической криптографией. Базовыми понятиями математической криптографии являются односторонняя функция, псевдослучайный генератор и доказательство с нулевым разглашением. Они позволяют строить новые математические модели, которые более адекватно отражают задачи криптографии. При этом возникают чисто математические постановки задач, а математическая криптография получает свой собственный аппарат и свои внутренние стимулы для развития. Естественно, что основные задачи математической криптографии изначально сложны, а некоторые из них по сути своей являются давно известными нерешенными математическими проблемами. Например, старая проблема нижних оценок вычислительной сложности — серьезные продвижения в ее решении позволят обосновать стойкость математических моделей большинства шифров. Вообще, математическая криптография — это наука, главным образом, о вычислительной сложности задач из некоторых специальных классов. Другой пример. Уже четверть века известно несколько гипотетических функций с секретом, основанных на задаче факторизации целых чисел. И до сих пор остается открытым вопрос о существовании еще хотя бы одной такой функции, основанной на какой-либо иной математической задаче.

Много важных теоретических и прикладных задач математической криптографии связано с изучением и обоснованием стойкости криптографических протоколов. В настоящее время выделено уже несколько десятков криптографических протоколов. Среди них есть и такие как:

- протокол распределенного конфиденциального вычисления,
- протокол голосования,
- система электронных платежей.

В этой бурно развивающейся и важной для приложений области математической криптографии еще многое не ясно. Отметим,

например, что для некоторых протоколов даже не сформулированы модели атак и угроз.

В последнее время большие надежды возлагаются на криптографию, использующую квантовый канал связи, или, как ее принято называть, квантовую криптографию. О квантовой криптографии пишут и в газетах, и в научно-популярной литературе. Международные научные коллективы проводят исследования и эксперименты по реализации квантового канала связи и периодически сообщают о своих очередных достижениях. Математики разрабатывают и обосновывают стойкость различных криптографических протоколов, главным образом протоколов генерации ключей с использованием гипотетического квантового канала связи. Это направление действительно очень перспективное, и для его реализации необходимы согласованные усилия физиков, математиков, криптографов.

Относительно новым направлением обеспечения безопасности информационных технологий является компьютерная стеганография. Разработанные в стеганографии методы скрытого «встраивания» одной информации в другую позволяют решать много новых задач. Так, например, имеется много публикаций по разработке идей построения электронных «водяных знаков» и электронных «отпечатков пальцев» методами стеганографии с использованием методов криптографии. Пока они носят чисто математический характер. Но если эти математические идеи удастся довести до технологии, то будут решены важные задачи защиты авторских прав и борьбы с незаконным распространением копий. Такие результаты очень нужны разработчикам программных продуктов.

Криптография как один из источников развития математики

В. А. Садовничий, В. А. Носов, В. В. Ященко

Любое общество не может гармонично развиваться без производства информации, ее накопления и обмена информацией. С другой стороны, в обществе всегда была и есть необходимость разграничивать круг лиц, для которых предназначена та или иная информация. Поэтому возникла и стала интенсивно развиваться криптография — наука о способах сокрытия информации от непосвященных лиц. Фактически криптография — ровесница письменности. Она в своем развитии прошла через этапы «криптография как искусство» и «криптография как ремесло» к этапу «криптография как наука». Последний этап начался совсем недавно — в сороковые годы двадцатого века. В это время почти одновременно два выдающихся ученых — Владимир Александрович Котельников в России и Клод Шеннон в США — заложили теоретико-информационные основы криптографии. Однако криптография, став наукой, продолжает оставаться и искусством, и ремеслом, поэтому в ней и в настоящее время присутствует больше практических наблюдений и рекомендаций, чем строгих теорем, что существенно отличает криптографию от математики. Но и математика, и криптография всегда развивались в тесном взаимодействии, взаимно обогащая друг друга.

В настоящей статье мы обсудим основную проблематику современной открытой криптографии. Следует подчеркнуть, что слова «открытая криптография» мы употребляем условно в смысле «открытые научные исследования в интересах криптографии». Криптография как наука едина, но в настоящее время одни научные направления в ней могут плодотворно развиваться только в открытом режиме, как составная часть соответствующих математических направлений, в то время как другие направления, слишком тесно связанные с приложениями, должны развиваться только в закрытом режиме в специализированных организациях.

Главная функция криптографии — защита информации. Длительное время криптография во всех странах развивалась под эгидой ведомств, отвечающих за безопасность связи и информации, и во многом представляла собой набор практических способов и рецептов защиты информации. С развитием средств связи — телеграфа, телефона, радио — менялся характер криптографии, а с началом применения электронных средств передачи информации задачи криптографии усложнились и расширились. В настоящее время, когда компьютерные технологии получили массовое распространение, проблематика криптографии преобразилась и пополнилась многочисленными задачами, которые не связаны непосредственно с засекречиванием информации. Перечислим некоторые из них: разработка систем электронной цифровой подписи, протоколов выборов, подписания контракта и идентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и систем электронных платежей.

Поэтому и значение криптографии в жизни общества продолжает возрастать. Недаром Дэвид Кан, автор фундаментального труда «Взломщики кодов», сказал: «Великая держава — это страна, которая владеет ядерными технологиями, ракетной техникой и криптографией». С этим нельзя не согласиться. А вот что сказал Ривест — один из соавторов системы шифра RSA: «Криптография является повивальной бабкой всех компьютерных наук». Еще более сильно выразились авторы фундаментального труда «Абстрактная прикладная алгебра» Р. Лидл и Г. Пильц — «Современная криптография может быть охарактеризована и как важная многомиллионодолларовая проблема, и как раздел прикладной математики». Они имеют в виду проблему получения доказуемых и адекватных нижних оценок стойкости шифров и, в частности, шифров с открытым ключом.

Как уже отмечалось, глубокое понимание математического характера криптографии началось с работ К. Шеннона. Его основополагающая работа «Математическая теория криптографии» в секретном варианте была выполнена в 1945 году, а рассекречена и опубликована в США в 1949 году. В 1963 году по инициативе Андрея Николаевича Колмогорова сборник работ К. Шеннона был издан и на русском языке с предисловием Андрея Николаевича. В 60-х годах были рассекречены и опубликованы результаты исследований немецкой шифрмашины «Энигма» и связанные

с этим результаты по решению уравнений в подстановках. В 70-х годах была опубликована революционная работа молодых американских ученых У. Диффи и М. Хеллмана «Новые направления в криптографии». С этого момента наблюдается лавинообразный рост числа публикаций по криптографии. Причины этого разнообразны. С одной стороны — постоянное расширение областей применения криптографии, о чем мы уже говорили. С другой стороны — новизна и привлекательность для ученых математических моделей и задач, которые возникают из потребностей криптографии. И наконец — именно в этот период формируются все атрибуты криптографии, как науки: возникают направления и научные школы со своей внутренней логикой развития, появляются специализированные международные журналы, закрепляется практика ежегодного проведения международных конференций.

Следует подчеркнуть, что формирование криптографии как науки проходило во второй половине XX-го века при определяющем влиянии математики. Вместе с тем криптография является наукой, использующей достижения и многих других наук. Например, результаты таких наук, как физика, теория связи, науки кибернетического цикла находят использование в криптографии и, с другой стороны, задачи и результаты криптографии влияют на проблематику этих наук.

В последние годы ряд криптографических идей и методов стал ядром новых междисциплинарных научных направлений, связанных с обеспечением информационной безопасности. В эту орбиту оказались вовлечены и юридические, и гуманитарные, и социальные науки.

Однако математический аппарат продолжает оставаться основным в криптографии. Ведь не случайно в многовековую историю криптографии вписано много имен видных математиков. Приведем лишь несколько наиболее ярких примеров.

Аристотель (384–322 до н. э.), древнегреческий ученый, участник Академии Платона, учитель Александра Македонского, охватил почти все доступные в то время знания. Перед математикой его заслуга состоит в том, что он дал первое систематическое изложение логики и теории доказательств. В криптографии известен как автор способа вскрытия шифра «сцитала».

Кардано Джероламо (1501–1576), итальянский математик. С его именем в математике связывают формулу Кардано для решения неполных кубических уравнений, он ввел мнимые корни

уравнений. В криптографии Кардано известен изобретением шифра, называемого «решеткой Кардано».

Виет Франсуа (1540–1603), французский математик. Он известен тем, что ввел в алгебру буквенные обозначения как для неизвестных величин, так и для коэффициентов. Его «формула Виета» связывает коэффициенты уравнения с его корнями. В криптографии Виет известен успешной дешифровальной работой при дворе короля Генриха IV.

Валлис Джон (1616–1703). Английский математик, один из основателей Лондонского математического общества. Внес значительный вклад в развитие интегрального исчисления. Валлис также успешно занимался дешифровальной работой.

Эйлер Леонард (1707–1783), швейцарский математик, большую часть жизни провел в России. Внес существенный вклад во все разделы математического анализа. Принимал участие в разработке российских государственных шифров.

Тьюринг Алан (1912–1954), английский математик, член Лондонского королевского общества. Выполнил цикл работ по математической логике и вычислительной математике. Автор формализации понятия алгоритма в виде абстрактной вычислительной машины (машины Тьюринга). Принимал непосредственное участие в дешифровании немецкой шифровальной машины Enigma. Автор концепции построения специализированной вычислительной машины для перебора ключей.

Шеннон Клод Эльвуд (1916–2001). В 1963 году Андрей Николаевич Колмогоров, представляя читателям русский перевод сборника работ К. Шеннона, писал в предисловии: «В наш век возрастающей дифференциации человеческих знаний Клод Шеннон является исключительным примером соединения глубины отвлеченной математической мысли с широким и в то же время совершенно конкретным пониманием больших проблем техники. Его в равной мере можно считать одним из первых математиков и одним из первых инженеров последних десятилетий».

Большой вклад в развитие отечественной криптографии внесли выпускники МГУ. Назовем лишь три имени.

Марков Андрей Андреевич (1903–1979). Разработал теорию нормальных алгоритмов, называемых теперь алгоритмами Маркова, и доказал алгоритмическую неразрешимость некоторых задач алгебры, в частности, неразрешимость проблемы тождества слов в конечно определенных полугруппах. Он имеет

многочисленные работы в области криптографии. Наиболее известна «теорема Маркова», которая классифицирует шифры, не распространяющие искажения.

Гельфонд Александр Осипович (1906–1968). Выпускник МГУ 1927 года. Решил седьмую проблему Гильберта о трансцендентности степени алгебраического числа в иррациональной алгебраической степени. Занимался решением многих криптографических задач, в частности, задачи дискретного логарифмирования.

Колмогоров Андрей Николаевич (1903–1987). Выпускник МГУ 1925 года. Внес существенный вклад во многие разделы математики. В криптографии нашли применение его работы по теории информации и теории вероятностей, в частности, его критерии случайности последовательностей.

Остановимся теперь коротко на тех направлениях математики, которые испытывали наибольшее влияние задач криптографии и в которых имеется много результатов с «криптографическими корнями».

Алгебра. Здесь в первую очередь следует назвать теорию конечных групп и особенно теорию групп подстановок, теорию конечных полей и особенно теорию уравнений над конечными полями, теорию рекуррентных последовательностей на алгебраических структурах, теорию универсальных алгебр.

Теория вероятностей. Теория вероятностей во многом возникла как прикладная наука. В связи с потребностями криптографии дополнительный стимул для развития получили теории случайных последовательностей и процессов, исследования по изучению свойств «случайных» комбинаторных объектов.

Комбинаторный анализ. Данная наука во многом развивалась в интересах криптографических приложений. Особенно это касается перечислительных проблем, связанных с подстановками, латинскими квадратами, дискретными функциями.

Теория чисел. В настоящее время здесь наблюдается подлинный бум в связи с широким распространением криптографических идей Диффи и Хеллмана, а также криптографической схемы RSA. Только благодаря криптографии любые продвижения в таких теоретико-числовых задачах, как «задача факторизации», «задача дискретного логарифмирования», «задача проверки простоты», теперь выплескиваются даже на газетные полосы.

Теория информации. Данная теория во многом базируется на тех же методологических подходах, что и криптография. Не случайно, основополагающие работы К. Шеннона по криптографии и теории информации выполнены практически одновременно. В своем дальнейшем развитии теория информации продолжает постоянно подпитываться проблематикой криптографии.

Теория кодирования. Основоположником теории кодирования также является К. Шеннон. Многие постановки задач в теории кодирования близки постановкам задач в криптографии, поэтому в криптографии широко применяются методы и результаты теории кодирования.

Дискретная математика. Данное направление получило развитие во многом благодаря потребностям компьютерных наук и криптографии. В частности, это относится к теории булевых функций, функций многозначной логики и теории автоматов. Именно с их помощью чаще всего описываются преобразования информации, реализуемые в шифраторах. Поэтому задачи анализа шифров являются одним из источников задач для дискретной математики.

Компьютерные науки. Началом данному направлению послужили идеи по формализации процесса алгоритмического вычисления и построению специализированной вычислительной машины для дешифрования. Данные идеи оказались плодотворными и при разработке современных суперкомпьютеров. Для большинства суперкомпьютеров, разработанных в XX-м веке, основным заказчиком и потребителем была криптография.

Более подробно хочется остановиться на двух направлениях, которые возникли под влиянием задач криптографии в последние 10–15 лет.

Направление «сложность алгоритмов и вычислений» — одно из направлений в компьютерных науках — сразу после своего возникновения получило криптографическую окраску. Теоретико-сложностной подход к оценке стойкости криптосистем широко применяется наряду с теоретико-информационным. Когда под влиянием идей Диффи и Хеллмана стали разрабатываться многочисленные криптографические протоколы, теоретико-сложностной подход стал основным для их изучения. Осмысление различных криптографических протоколов и методов их построения привело в 1985–1986 гг. к появлению двух плодотворных математических моделей — интерактивной системы доказательства

и доказательства с нулевым разглашением. На основе этих моделей в математической логике и теории сложности в настоящее время разрабатывается математический аппарат, наиболее адекватно отражающий проблематику «новой криптографии».

Идея использовать в интересах криптографии законы квантового мира давно витала в воздухе. Но лишь в последние годы она приобретает реальные очертания в виде концепций квантовых коммуникаций и квантовых вычислений. Разработка этих концепций потребовала объединения усилий высококвалифицированных специалистов из разных направлений — криптографов, физиков, математиков, компьютерщиков. Реализация идей квантового компьютера и квантовых коммуникаций приведет к революционным изменениям в ряде областей науки и техники и может серьезно повлиять на состояние безопасности страны, в частности, информационной безопасности.

Научно-методологические проблемы квантовых вычислений

В. А. Садовничий, А. В. Корольков

Прелесть квантовых вычислений заключается в том, что при измерении состояний, представимых в виде суперпозиции чистых состояний, квантовые вычисления производятся как бы одновременно над всеми составляющими (это явление носит название квантового параллелизма).

Из выступления на семинаре в МГУ.

Проблематика квантовых вычислений и квантовых компьютеров стала в последние годы весьма актуальной и востребованной. Причиной этому стали научные открытия и технологические достижения, сделавшие принципиально возможными решение целых классов сложнейших вычислительных задач, имеющих стратегическое значение и прямое отношение к критически важным технологиям, таким как криптографические и ядерно-физические.

К исследованиям в области квантового компьютинга привлечены сегодня серьезные научные силы многих стран, включая Россию, где в 1999 году впервые был учрежден международный научный журнал «Квантовые компьютеры и квантовые вычисления». Ведется незримая «гонка квантовых вооружений», направленная на создание полномасштабного квантового компьютера, позволяющего решать такие задачи, для которых потребовались бы сотни лет работы даже при объединении вычислительных мощностей всех существующих на сегодня компьютеров из списка наиболее мощных TOP100.

Под эгидой МГУ им. Ломоносова и Академии криптографии РФ недавно был выполнен цикл теоретических исследований, позволивший провести анализ и систематизацию современных результатов исследований в области квантовых вычислений,

на основе которых определены направления перспективных разработок, имеющих приоритетное значение.

Основными целями современных исследований в области квантового компьютинга являются:

- разработка подходов к построению эффективных квантовых алгоритмов решения вычислительно сложных и актуальных для конкретных применений математических и физических задач (в частности, криптографических задач и задач моделирования поведения квантовых объектов);
- разработка подходов к построению прототипов технических средств, реализующих квантовые алгоритмы — квантовых вычислителей (КВ).

Анализ показал, что в последние годы одними из наиболее обсуждаемых проблем *в математической области* стали проблемы теории сложности квантовых вычислений, проблемы расширения класса эффективных квантовых алгоритмов и проблемы обеспечения устойчивости квантовых вычислений применительно к различным моделям КВ, в частности, за счет использования методов квантовой коррекции ошибок.

При этом среди новых направлений работ, которые должны быть выполнены в ближайшем будущем в первую очередь, следует, на взгляд авторов, выделить следующие:

- исследование подходов к учету погрешностей квантовых вычислений при реализации квантовых алгоритмов;
- исследование подходов к созданию методов и языков квантового программирования;
- исследование подходов к организации «распределенных» квантовых вычислений и обеспечения квантового информационного обмена с помощью квантовых каналов связи между отдельными квантовыми вычислителями (в том числе, обмена с квантовой памятью) в квантовой информационно-вычислительной среде (квантовый Интернет).

Одними из наиболее обсуждаемых проблем *в физико-технической области* за последние годы стали проблемы конструирования элементной базы квантовых компьютеров. Эти исследования, находившиеся более 10 лет в стадии экспериментальных исследований по созданию физических и технологических основ

отдельных вычислительных элементов, уже сейчас начали выходить на уровень проектирования прототипов КВ, выполняющих отдельные квантовые алгоритмы.

К сожалению, существующие квантовые системы еще не способны обеспечить надежные вычисления, так как они либо недостаточно управляемы, либо очень подвержены влиянию шумов. Однако физических запретов на построение эффективного квантового компьютера нет, необходимо лишь преодолеть технологические трудности.

Прототипы квантовых компьютеров существуют уже сегодня. Правда, пока что экспериментально удается собирать лишь небольшие регистры, состоящие всего из нескольких квантовых битов.

В 2002 году фирма IBM анонсировала, что в их научной лаборатории под руководством И. Чанга осуществлена первая работающая реализация алгоритма Шора разложения числа на множители (Shor's factoring algorithm). Используя свои разработки, специалисты в IBM построили квантовый компьютер с семью квантовыми битами. На данный момент это — одна из самых сложных разработок в данной области. Этот компьютер успешно решил задачу по разложению числа 15 на множители, получив в результате 5 и 3. Несмотря на такой очевидный результат, данный алгоритм является одной из самых сложных демонстраций квантовых вычислений на сегодняшний день. Этот же прототип квантового компьютера используется для решения некоторых математических задач криптографии, например, нахождения периода функций. Квантовый компьютер способен решать задачи в один цикл, в то время как традиционному компьютеру для этих же целей понадобились бы многократные циклы.

Компания Hewlett-Packard и Технологический институт штата Массачусетс (США) с 2001 года работают над рассчитанным на четыре с половиной года проектом стоимостью 2,5 миллиона долларов, направленным на разработку квантовых информационных систем, в частности, над созданием компонент квантового компьютера. Приход компании Hewlett-Packard в новую для себя область деятельности может означать начало нового этапа развития квантовой электроники. Квантовые информационные системы, включая квантовые компьютеры и молекулярную электронику, представляют собой метод обработки информации, коренным образом отличающийся от существующего. Согласно некоторым

прогнозам, ожидается, что в течение ближайших 10 лет молекулярная электроника полностью заменит существующие технологии на основе кремния. Однако, на наш взгляд, современные технологические заделы в полупроводниковой микроэлектронике и наноэлектронике позволят обеспечить совместное сосуществование этих направлений гораздо более длительный период.

Среди новых направлений работ, которые должны быть выполнены в ближайшем будущем, в первую очередь, следует, на взгляд авторов, выделить следующие:

- моделирование квантовых кубитов и квантовых регистров, функционирующих в соответствии с заданным квантовым алгоритмом;
- преодоление проблем декогерентизации квантовых состояний в процессе вычислений с целью обеспечения возможности реализации более сложных квантовых алгоритмов;
- поиск путей построения квантовых вычислительных структур большой размерности (с числом кубитов более 1000) и создания масштабируемых квантовых вычислителей;
- создание экспериментального прототипа специализированного квантового компьютера, допускающего внешнее программное управление и предназначенного для решения одной из известных сложных вычислительных задач, имеющих приложение в ряде областей практической жизни;
- доказательство принципиальной возможности реализации и определение технических и технологических требований к экономически выгодному универсальному квантовому компьютеру.

Кубиты для квантового компьютера

Сегодня разработка практической реализации квантовых вычислений идет по трем основным направлениям: ядерный магнитный резонанс (ЯМР), твердое тело и ионные ловушки.

Самая изученная из этих технологий — ЯМР, где кубитами являются атомные ядра, находящиеся в одной молекуле и общающиеся друг с другом путем спиновых взаимодействий. Из такой молекулы вы можете сделать маленький квантовый компьютер.

Собственно, технология ЯМР и есть квантовое вычисление, хотя она известна уже десятки лет и применяется совсем в других целях. Проблема в том, что эта технология вряд ли масштабируема. В принципе можно использовать и очень длинные молекулы, но одновременно работать более чем с десятью спинами очень сложно. А так как исследования квантовых вычислений на основе ЯМР ведутся уже двадцать с лишним лет, здесь трудно ожидать больших скачков.

Твердотельной технологией сейчас занимаются очень многие, в том числе и в России. Проблема в том, чтобы получить сцепленные электроны в твердом теле — то есть в материале, который любят производители компьютеров. Как только будет создан работающий прототип реализации квантовых вычислений в твердом теле, в области квантового компьютинга может начаться взрывное развитие.

В ионных ловушках можно в принципе удерживать много ионов. Если загнать в ловушку «строку» из большого числа ионов, возникает их взаимодействие в квантовом режиме. Сейчас пытаются получить сцепленные наборы из нескольких ионов, которые можно будет использовать для простых квантовых вычислений. Пока это удалось для двух ионов. Теоретически можно получить строку из 100–200 ионов (кубитов). Это уже очень много, так как размерность фазового пространства будет 2 в степени количества ионов. Такую систему можно считать настоящим квантовым компьютером.

В твердом теле, в принципе, возможно то же самое, но на практике в кристалле всегда есть множество неоднородностей, которые портят все дело. Если бы удалось получить идеальный кристалл и охладить его до состояния минимальной энергии (ground state), такая среда была бы очень удобна для создания сцепленных электронов. Но на это потребуется по крайней мере несколько лет.

Существует несколько идей и предложений, как сделать надежные и легко управляемые квантовые биты.

В Институте теоретической физики им. Л. Д. Ландау РАН предложено собирать квантовые регистры из миниатюрных сверхпроводниковых колец. Каждое кольцо выполняет роль кубита, а состояниям 0 и 1 соответствуют направления электрического тока в кольце — по часовой стрелке и против нее. Переключать такие кубиты можно магнитным полем. Похожий

подход развивается в Массачусетском технологическом институте и Делфтском технологическом университете, где составная часть будущих квантовых компьютеров — квантовые логические элементы — представляют собой микроскопические петли из сверхпроводящего материала. Электрический ток в таких петлях подчиняется квантовым законам. Поэтому два противоположных направления тока в петле могут не только представлять состояния «0» и «1», но возможна также суперпозиция этих состояний, что дает возможность манипулирования так называемым кубитом. По мнению исследователей, главное преимущество их подхода состоит в простоте производства больших систем из сверхпроводящих петель по существующим технологиям, а также возможность создания квантовой связи между ячейками с помощью дополнительных петель. Управление отдельными ячейками можно осуществлять с помощью магнитных микроволновых импульсов, а считывание с них информации — с помощью сверхпроводящих магнетометров.

В Физико-технологическом институте (ФТИ) РАН группа под руководством академика К. А. Валиева предложила два варианта размещения кубитов в полупроводниковых структурах. В первом случае роль кубита выполняет электрон в системе из двух потенциальных ям, создаваемых напряжением, приложенным к миниэлектродам на поверхности полупроводника. Состояния 0 и 1 — положения электрона в одной из этих ям. Переключается кубит изменением напряжения на одном из электродов. В другом варианте кубитом является ядро атома фосфора, внедренного в определенную точку полупроводника. Состояния 0 и 1 — направления спина ядра вдоль либо против внешнего магнитного поля. Управление ведется с помощью совместного действия магнитных импульсов резонансной частоты и импульсов напряжения.

Рассмотрим это направление исследований более подробно.

Как сконструировать элементы твердотельных квантовых компьютеров?

В целях поиска путей практической реализации квантовых вычислителей российскими исследователями был проведен анализ методов измерения квантового состояния одиночных кубитов и ансамблевых кубитов. Показано преимущество ансамблевых подходов к построению квантовых компьютеров. Рассмотрение

известных вариантов квантовых компьютеров с использованием ядерного магнитного резонанса (ЯМР-КК) на молекулах органической жидкости показало, что предельное количество кубитов в них ограничено числом 20–30.

Еще в 2002 году во ФТИ РАН были определены условия, при которых может быть создан полномасштабный ЯМР квантовый компьютер с числом управляемых кубитов не менее 1000. Это может быть достигнуто только при очень низких спиновых температурах (менее одной десятой градуса Кельвина) в твердотельных структурах. В этом случае сигнал ЯМР оказывается независящим от числа кубитов (не происходит его экспоненциального уменьшения как в жидкостных вариантах), и не требуется никакой специальной процедуры инициализации состояний спинов. Предложен вариант прототипа квантового компьютера на основе кремниевой структуры с системой чередующихся полосковых затворов шириной менее 10 нм с правильной двумерной периодической структурой из донорных атомов фосфора. Измерение состояний ядерных спинов-кубитов на выходе ансамблевого квантового компьютера может быть осуществлено с помощью стандартных ЯМР-методов.

Использование ансамблевых подходов в реализации полномасштабных ЯМР-КК имеет следующие преимущества по сравнению с подходами, основанными на индивидуальном обращении к кубитам:

- в случае варианта с полосковыми затворами отпадает необходимость использования тонких высокочувствительных устройств для измерения состояний отдельных спинов-кубитов;
- в результате усреднения по ансамблю неточностей расположения доноров под затвором и геометрических параметров самих затворов снижаются требования к точности изготовления соответствующих наноструктур;
- вариант ансамблевого квантового клеточного автомата не требует создания наноструктур с многочисленными затворами, в результате чего существенно упрощается конструкция квантового регистра и исчезает механизм декогеренции, связанный с электрическими шумами.

Учеными из ФТИ РАН было проведено исследование проблем конструирования физической структуры твердотельных

квантовых компьютеров на основе атомов ^{31}P и ^{28}Si с учетом реализации процедур коррекции квантовых ошибок. Предложен вариант конструктивного исполнения ансамблевого КВ в виде двумерной решетки с полосковыми затворами, реализующими многокубитовый квантовый регистр (рис. 1).

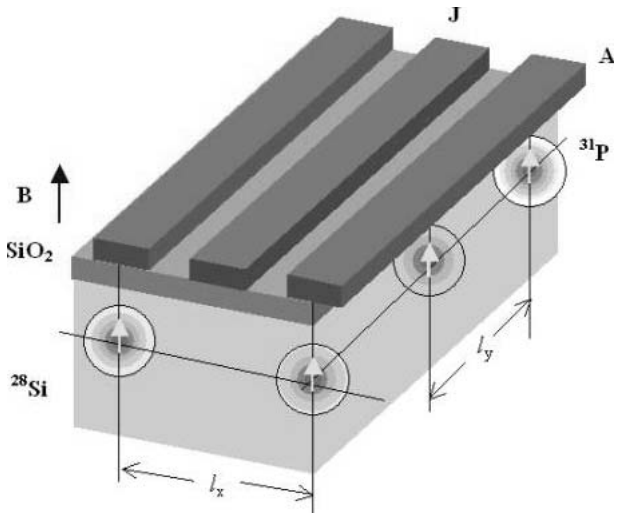

Рис. 1. Вариант конструктивного исполнения ансамблевого КВ.

Данная схема является обобщением схемы Кейна на ансамблевый вариант с полосковыми затворами. Для инициализации состояний ядерных спинов предложен так называемый solid-state эффект в технологии ENDOR, в которой ядерные спины можно почти полностью поляризовать, или, что то же самое, охладить до спиновых температур ~ 1 mK.

В ходе анализа предложенного варианта КВ было показано, что можно добиться исключения случайных аналоговых фазовых ошибок в базисных состояниях квантового регистра, а оставшиеся не усредненными дискретные ошибки могут быть исправлены с помощью квантовых корректирующих кодов.

В предложенном варианте конструктивного исполнения КВ измерение состояний ядерных спинов-кубитов на выходе ансамблевого квантового компьютера может быть осуществлено с помощью стандартных ЯМР методов. При этом впервые

показано, что необходимость измерения состояний всех кубитов регистра в процессе выполнения квантовых логических операций с предельно высокой точностью не возникает, а измерение сигнала с помощью стандартной ЯМР методики от $L \sim 10^3$ кубитов может быть достигнуто при количестве компонентов ансамбля $N > 10^5$.

Основные преимущества кремниевых ЯМР квантовых компьютеров с донорными атомами ^{31}P в качестве кубитов, по сравнению с компьютерами на электронных состояниях, состоят в следующем.

1. Ядерные спины-кубиты характеризуются очень большими временами релаксации при низких температурах (часы).
2. Для управления кубитами и измерения выходного сигнала в ансамблевом варианте может использоваться хорошо разработанная техника ЯМР.
3. Для инициализации квантовых состояний кубитов и для подавления декогерентизации в полупроводниковых ЯМР регистрах может быть использована техника двойного электрон-ядерного резонанса и техника ЯМР-спектроскопии высокого разрешения.
4. Создание ЯМР ансамблевых квантовых структур может быть осуществлено современными методами сверхтонкой нанотехнологии.

Таким образом, следует считать, что важные, ближайшие перспективы открываются именно перед направлением кремниевых ЯМР квантовых компьютеров с донорными атомами ^{31}P.

Можно ожидать, что в будущем появятся также комбинированные варианты твердотельных квантовых компьютеров, использующих, например, в одной структуре и ядерные спины, и квантовые точки с электронными спинами, а также комбинированные методы обращения к кубитам с использованием двойного электронно-ядерного магнитного резонанса.

Важнейшими пока остаются проблемы подавления процессов декогерентизации квантовых состояний, исправления случайных ошибок, организации помехоустойчивых квантовых вычислений, а также проблема измерения конечного квантового состояния. Вместе с тем, их решение для ЯМР квантовых компьютеров облегчается при ансамблевом подходе.

Фатальна ли проблема погрешностей квантовых вычислений для реализации квантовых алгоритмов?

К сожалению, на сегодняшний день не известно ни одной модели квантового вычисления, которая считалась бы перспективной для реализации и имела удовлетворительное решение проблемы устойчивости вычислений к сбоям. Проблема квантового вычисления, устойчивого к ошибкам, стала центральной проблемой современных исследований в области квантового компьютинга. Анализ показал, что теоретически эта проблема может быть решена — *надежное квантовое вычисление возможно*. Однако условия, при которых оно возможно, оказываются весьма жесткими. Во-первых, надежное квантовое вычисление возможно только при очень малом уровне шума. Во-вторых, показана невозможность надежного последовательного квантового вычисления, т. е. физические реализации квантовых компьютеров должны обеспечивать максимальный параллелизм. В-третьих, надежное квантовое вычисление невозможно в чисто унитарной модели КВ: как минимум требуется приготавливать кубиты в известном состоянии в процессе вычисления и удалять часть кубитов.

В результате последних исследований показано, что часть из этих условий может быть ослаблена, а часть — неустранима. Например, необходимость постоянной подпитки «свежими» кубитами, приготовленными в стандартном состоянии, оказывается особенно существенной в моделях КВ, где кубиты расположены на прямой или на плоской решетке, причем взаимодействие разрешено только между соседними кубитами. Добавление в такие структуры «свежих» кубитов может оказаться весьма трудной задачей.

Перспективными в этой связи можно считать новые подходы к построению квантовых алгоритмов, реализуемых упрощенными физическими методами. Актуальность этой задачи обуславливается тем, что технически сложно выполнять двухкубитные преобразования в процессе квантовых вычислений, а однокубитные преобразования выполнять существенно проще. Так, например, может быть полезен подход, реализующий управление эволюцией квантовой системы под воздействием только однокубитных преобразований. Основная трудность модели с однокубитным управлением состоит в том, что двухкубитное взаимодействие

происходит неконтролируемым образом, и для производства вычислений нужно создать и применять методы коррекции «нежелательных» преобразований с помощью однокубитных преобразований.

В настоящее время пока не преодолены ограничения на возможности исправления ошибок в КВ, даже с использованием квантовых корректирующих кодов. Вместе с тем, недавно было показано, что всякий квантовый код должен быть схемой разделения секрета и описаны подходы к получению полиномиальных квантовых кодов, базирующиеся на известных идеях, использующихся в криптографических протоколах конфиденциального вычисления с полиномиальной схемой разделения секрета.

Помимо практической выгоды — распараллеливания вычислений, квантовый параллелизм является и причиной уязвимости квантовой системы к внешним воздействиям. Так как состояние системы может быть результатом суперпозиции нескольких состояний, важно, чтобы оно было изолировано от паразитного внешнего воздействия, приводящего к изменению результирующего состояния и, соответственно, искажающего результат квантовых измерений или, если будет угодно, вычислений.

Таким образом, очень важно сохранить когерентность состояний кубита. Когерентные состояния очень чувствительны к внешним воздействиям, будь то измерение или случайное воздействие, например, шальной квант электромагнитного поля. От последних, кстати, изолироваться практически невозможно, так как всегда существуют так называемые нулевые флуктуации поля, проявляющиеся, в частности, в эффекте Казимира (эффект возникновения силы притяжения между зеркалами резонатора, вызванный разницей в спектрах нулевых колебаний поля вне и внутри резонатора).

Для решения этой проблемы еще в 1995 году были придуманы способы коррекции ошибок, а в 1998 году осуществлена первая их практическая реализация. Основной идеей предложенного метода коррекции ошибок было разложение смешанного состояния кубита на составляющие (своего рода спектр) для сравнения состояний до вычисления и после. Зная спектр состояний кубита, можно приготовить аналогичное состояние в любой момент, пока, конечно, нам не понадобится что-то с кубитом сделать. Этот процесс — разложение состояния кубита на спектр составляющих и восстановление когерентного состояния, аналогичен процессу

обновления содержимого динамической памяти в компьютере. На данный момент время декогерентизации в прототипах квантовых чипов не превышает 1 мкс, следовательно, для поддержания состояния кубита его необходимо обновлять миллион раз в секунду, что требует немалых затрат. По мнению некоторых специалистов, для квантовых вычислений требуется время не меньшее 1 мс, то есть на три порядка больше, чем то, что достигнуто сейчас.

На графике рис. 2 приведена зависимость потребляемой энергии от времени декогерентизации для теоретического квантового чипа, используемого для взлома криптографического кода AES с 1024-разрядным ключом. Некоторые расчеты показывают, что даже чипы с временем декогерентизации порядка 10 мкс будут рассеивать более 100 МВт. В то же время, по этим же расчетам, при времени декогерентизации 1 мс такой квантовый чип будет потреблять около 1 Вт.

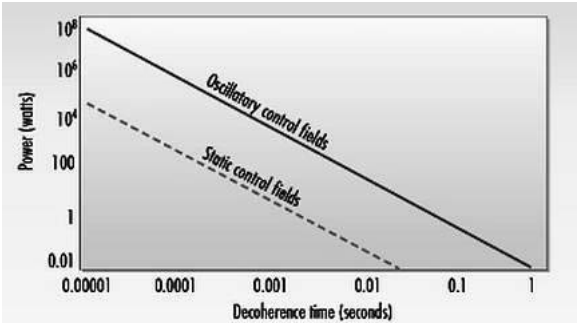

Рис. 2. Зависимость потребляемой энергии от времени декогерентизации для теоретического квантового чипа, используемого для взлома криптографического кода AES с 1024-разрядным ключом.

Недавно было доказано утверждение, что количество энергии, затрачиваемой на коррекцию ошибок, обратно пропорционально времени декогерентизации.

Возможные выходы из ситуации:

- использовать спин электрона, с которым ученые умеют работать достаточно хорошо, но связав его со сверхпроводящим квантово-интерференционным устройством (SQUID, устройство с джозефсоновским контактом), в котором возможно достижение достаточно большого времени декогерентизации;
- использовать атомы с хорошо изолированными энергетическими уровнями, характеризующимися большими временами жизни.

Несмотря на то, что с математической точки зрения проблема надёжного квантового вычисления решена, существующие ограничения, которые накладываются на такие вычисления, оказываются очень сильными. Существующие на сегодня оценки критической интенсивности ошибок (от 10^{-6} до 10^{-3}) вряд ли будут существенно повышены. Пути возможного снижения этих ограничений требуют дальнейших серьезных исследований и усложнения модели квантового компьютера. Следует отметить при этом, что подходы к реализации квантового компьютера, допускающие возможность промежуточных измерений и использования классических вычислений на результатах этих измерений, имеют значительное преимущество перед такими подходами, в которых измерения допускаются только в конце. Вероятно, наиболее перспективным направлением исследований является анализ различных нестандартных моделей квантовых вычислений одновременно как с точки зрения возможности их реализации, так и на предмет существования эффективных методов исправления ошибок.

Таким образом, результаты современных исследований позволяют с большой долей уверенности предположить, что в самом недалеком будущем — лет через 5–10 — эффективный квантовый компьютер будет создан, но для его создания потребуются серьезные усилия специалистов.

Какие алгоритмы будут реализованы на квантовых компьютерах?

В настоящее время показано, что на квантовом компьютере принципиально можно решить любую математическую задачу. Вопрос в том, насколько эффективно по времени будет это решение. Известные на сегодня эффективные квантовые алгоритмы можно условно разделить на две группы: дающие экспоненциальный выигрыш (например, алгоритм Шора) и дающие квадратичный выигрыш (например, алгоритм Гровера).

В связи с тем, что класс задач, решаемых квантовыми алгоритмами за полиномиальное время, пока не удается расширить очень существенно, большое внимание во всем мире уделяется анализу алгоритма Шора и других полиномиальных алгоритмов с целью выявления общности и важнейших свойств этих алгоритмов, а также соответствующих задач, позволяющих добиться полиномиальности.

Систематизация алгоритмов типа Шора для задач алгебры может быть основана на том, что алгоритм Шора содержит принципиальное ядро и окружение, позволяющее сводить исходную задачу к этому ядру. В алгоритме Шора таким ядром является алгоритм нахождения периода относительно возведения в степень, а именно, нахождение для данных взаимно простых натуральных чисел a и q наименьшего положительного t такого, что $a^t \equiv 1 \pmod{q}$. Поскольку задача нахождения периода является частным случаем задачи о скрытой подгруппе, большое внимание современными исследователями уделяется изучению особенностей квантовых алгоритмов решения этой задачи, а также связанной с ней задачи об изоморфизме графов.

В результате анализа алгоритмов Шора и Саймона, также сводящегося к задаче о скрытой подгруппе, можно выделить их важные общие части и различия. Так, эти алгоритмы используют идею перехода от группы G к некоторому двойственному объекту, действия с двойственным объектом и перехода обратно. При этом в них используются квантовые преобразования Фурье на группе G. Основным ядром в этих алгоритмах является квантовая подпрограмма, которая по заданному отображению абелевой группы в конечное множество строит специальное вероятностное распределение на группе характеров исходной группы. Анализ показал, что в настоящее время известны три варианта квантовых алгоритмов для задачи о скрытой подгруппе. Два из них находят порядок максимальной циклической подгруппы в скрытой факторгруппе. Третий находит саму скрытую подгруппу.

Интересные результаты дает рассмотрение особенностей квантовых алгоритмов, содержащих различные интегральные преобразования. Показано, что для них оказываются полезными некоторые принципы построения классических быстрых ортогональных преобразований. На сегодня известны рекуррентные структуры на основе квантовых вентилей для квантовых алгоритмов, реализующих следующие ортогональные преобразования:

- преобразование Фурье;
- преобразование Уолша—Адамара;
- Слэнт-преобразование;
- преобразование Хартли.

При этом все эти преобразования требуют для своей реализации не более $O(n^2)$ операций на квантовом компьютере с квантовым регистром длины n.

Недавно была предложена квантовая реализация Wavelet-преобразования и описана возможность его эффективного использования в алгоритме Шора взамен квантового Фурье-преобразования.

Исследователями выделен также ряд задач алгебры, в которых применение квантового преобразования Фурье дает значительное ускорение. Среди них: задача о сдвиге, задача о скрытом смежном классе, задача о сдвигах характеров конечных полей. Рассмотрены особенности решения задач, связанных с задачей о скрытой подгруппе, когда исходная группа не является абелевой.

Интересны с точки зрения криптографических приложений исследования по оценке трудоемкости квантового алгоритма дискретного логарифмирования Шора для случая группы точек эллиптической кривой, определенной над конечным простым полем.

Сегодня можно утверждать также, что в эффективные квантовые алгоритмы может быть трансформирован ряд современных алгоритмов в области алгебраической геометрии и алгебраической теории чисел. Например, были рассмотрены квантовые алгоритмы, основанные на арифметических свойствах эллиптических и гиперэллиптических кривых над конечными полями. В ходе анализа проблемы дискретного логарифма в группах Якоби гиперэллиптических кривых был предложен способ усовершенствования алгоритма факторизации с использованием сумм Якоби за счет применения субэкспоненциального по трудоемкости алгоритма Ленстры на этапе предварительных вычислений. Эти результаты послужили основой для предположения о том, что эффективными квантовыми реализациями могут обладать и итерационные алгоритмы, использующие эллиптические интегралы. Недавно был проведен анализ особенностей реализации итерационных алгоритмов, использующих эллиптические интегралы и метод арифметико-геометрического среднего. Описан высокоэффективный метод построения итерационных алгоритмов,

использующий полные эллиптические интегралы, тэта-функции и модулярные уравнения. Этот метод позволяет с высокой точностью вычислять значения различных алгебраических функций, а также функций математической физики. Сформулированы основы этого метода и продемонстрированы его возможности для вычисления числа π. Сделан вывод, что можно ожидать выигрыша в трудоемкости от применения квантовых алгоритмов, построенных с использованием итерационных процедур на базе полных эллиптических интегралов, тэта-функций и модулярных уравнений.

Таким образом, в рамках сегодняшних представлений, первые квантовые компьютеры будут, скорее всего, специализированными вычислителями, «заточенными» на решение конкретных классов сложных в вычислительном отношении задач. На расширение круга этих задач, а, значит, и на повышение экономической эффективности самих квантовых компьютеров, должны быть направлены усилия современных исследователей.

Заглянем в будущее

Попробуем представить, как мог бы выглядеть будущий квантовый компьютер. Вероятно, большой (масштабируемый) компьютер будет содержать тысячи управляющих элементов, действующих локально на каждый кубит. Каким образом могло бы осуществляться это воздействие? Скорее всего, с помощью электрических импульсов, подаваемых на микроэлектроды, подведенные к кубитам. Возможно также оптическое управление пучками света, сфокусированными на кубитах. Однако в этом случае трудно избежать паразитного воздействия на соседние кубиты дифракционных краев сфокусированного пучка. Что касается электрических методов, то они уже давно и широко применяются в микроэлектронике для управления классическими логическими элементами. Поэтому их использование представляется наиболее перспективным и для создания масштабируемых квантовых компьютеров. (Возможно, конечно, что в результате какого-нибудь технологического прорыва появится еще и третий вариант. Однако революционные открытия трудно поддаются прогнозу.)

Таким образом, весьма возможно, что в перспективе квантовые компьютеры будут изготавливаться с использованием

традиционных методов микроэлектронной технологии и содержать множество управляющих электродов, напоминая современный микропроцессор. Для того чтобы снизить уровень шумов, критически важный для нормальной работы квантового компьютера, первые модели, по всей видимости, придется охлаждать жидким гелием. Вероятно, первые квантовые компьютеры будут громоздкими и дорогими устройствами, не умещающимися на письменном столе и обслуживаемыми большим штатом системных программистов и наладчиков оборудования. Доступ к ним получат сначала лишь государственные структуры, затем крупные коммерческие организации. Но примерно так же начиналась и эра обычных компьютеров.

А что же станет с классическими компьютерами? Отомрут ли они? Вряд ли. И для классических, и для квантовых компьютеров найдутся свои сферы применения. Хотя, по всей видимости, соотношение на рынке будет все же постепенно смещаться в сторону последних.

Внедрение квантовых компьютеров, по-видимому, в далекой перспективе может привести к решению принципиально нерешаемых классических задач, а в ближайшей перспективе — серьезно ускорит некоторые сложные вычисления. Кроме того, станет возможна квантовая связь — передача кубитов на расстояние, что приведет к возникновению своего рода квантового Интернета. Квантовая связь позволит обеспечить защищенное (законами квантовой механики) от подслушивания соединение всех желающих друг с другом. Информация, хранимая в квантовых базах данных, будет надежнее защищена от копирования, чем сейчас. Фирмы, производящие программы для квантовых компьютеров, смогут уберечь их от любого, в том числе и незаконного, копирования. Квантовые компьютеры станут основой для построения теоретически безопасной компьютерной связи.

О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности

В. П. Шерстюк

Человечество вплотную подошло к рубежу, за которым начинается новый этап его развития, получивший название «информационного общества». Как неоднократно отмечал Президент Российской Федерации В. В. Путин, мы не имеем права проспать разворачивающуюся в мире информационную революцию. Она предопределяет, с одной стороны, дальнейшую интенсификацию развития мировой информационной сферы, обострение конкуренции за мировое лидерство в этом процессе, а с другой — делает информационную сферу все более привлекательной для оказания экономического, политического, военного или культурного давления на другие страны.

В современных условиях информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности российского государства. Обусловлено это, прежде всего, быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на политику, хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей стали в настоящее время решающими и всеохватывающими.

Практика государственного строительства показала, что стране необходим программный документ, определяющий политику государства в области обеспечения информационной безопасности. Таким документом стала Доктрина информационной безопасности Российской Федерации, одобренная Советом Безопасности и утвержденная Президентом Российской Федерации 9 сентября 2000 года. В ней впервые сформулированы

национальные интересы России в информационной сфере, определены угрозы информационной безопасности и пути противодействия этим угрозам.

Одним из факторов, способствующих повышению опасности угроз информационной безопасности, является дефицит квалифицированных кадров, обусловленный снижением эффективности системы образования и воспитания. Подготовка квалифицированных кадров в области информационной безопасности и информационных технологий осуществляется по двум основным направлениям — технологическому и гуманитарному.

Технологическая составляющая информационной безопасности включает в себя проблемы, связанные с развитием индустрии информатизации, обеспечением потребностей внутреннего рынка ее продукцией и выходом этой продукции на мировой рынок, а также с обеспечением безопасности информационных и телекоммуникационных систем.

Гуманитарная составляющая включает в себя большую совокупность проблем, связанных с соблюдением конституционных прав и свобод граждан в области духовной жизни и информационной деятельности, обеспечением духовного обновления России. Нельзя не отметить, что технологическая составляющая информационной безопасности разработана более тщательно и глубоко, в то время как гуманитарная составляющая — гораздо слабее.

Если на сегодняшний день существует уже более 100 вузов России, осуществляющих подготовку кадров в технологической составляющей, имеется 7 государственных образовательных стандартов и разработанных на их базе основных образовательных программ по вышеназванным специальностям, то по гуманитарной составляющей такие стандарты пока не созданы и специальности не утверждены.

Подобное положение не позволяет обеспечить реализацию Доктрины информационной безопасности и поэтому развитие гуманитарной составляющей системы обеспечения информационной безопасности должно сегодня стать приоритетным направлением приложения наших усилий.

В числе пионеров разработки проблем обеспечения информационной безопасности, относящихся к гуманитарной составляющей, находится Московский государственный университет. Решением секции по информационной безопасности научного совета при Совете Безопасности Российской Федерации Университет

определен головной организацией по научным проблемам обеспечения информационной безопасности, имеющим гуманитарный характер. На наш взгляд, МГУ обладает необходимым потенциалом, чтобы стать головной организацией и в области подготовки соответствующих специалистов с высшим образованием. Такая постановка проблемы поддержана и Ректором университета академиком Садовничим В. А.

Определенным шагом на пути решения данной задачи явилось создание в Московском университете в 1999 г. кафедры информационной безопасности, которой поручено стать в университете организационным началом развития научных исследований и учебного процесса по проблемам обеспечения информационной безопасности. За четыре года после создания кафедры информационной безопасности проделана немалая работа по организации в МГУ учебного процесса по проблематике информационной безопасности.

Отмечу лишь наиболее значимые мероприятия:

- При активном участии руководства МГУ и сотрудников кафедры информационной безопасности в декабре 1999 г. на коллегии Миннауки России утвержден новый перечень специальностей ВАКа, в который включена специальность 051319 «Методы и системы защиты информации. Информационная безопасность».
- В марте 2000 г. на коллегии Минобразования России утвержден новый перечень специальностей высшего профессионального образования, в который включен блок 075000 из 6 специальностей в области информационной безопасности.
- Положительно решен вопрос об открытии на факультете военного обучения МГУ военно-учетных специальностей в области информационной безопасности.
- В марте 2000 г. начал работать ежемесячный межведомственный междисциплинарный семинар по научным проблемам информационной безопасности. При большой активности участников уже проведено 17 заседаний семинара по различным аспектам технологических и гуманитарных проблем информационной безопасности; в процессе подготовки и проведения семинаров вокруг кафедры сформировался круг ученых и специалистов,

заинтересованных в развитии проблематики информационной безопасности; большое число встреч и дискуссий, проведенных на кафедре, позволило выработать целый ряд плодотворных научных и организационных предложений, которые реализуются как внутри МГУ, так и в других ведомствах, включая аппарат Совета Безопасности Российской Федерации.

- В соответствии с протоколом, подписанным Генеральным директором ФАПСИ и ректором МГУ, с сентября 2000 г. в МГУ открыты две новые специализации: на мехмате — 010123, «математические методы защиты информации», отв. — член-корр. РАН Нестеренко Ю. В.; на ВМиК — 010213.01, «математическое и программное обеспечение защиты информации», отв. — зав. кафедрой профессор Алексеев В. Б. Открытие этих специализаций для базового образования позволяет теперь вести все формы дополнительного образования в этом направлении в университете.

  В рамках этого соглашения проводятся научно-исследовательские разработки, представляющие взаимный интерес.

  Хорошо бы, чтобы полезный опыт взаимодействия между МГУ и ФАПСИ распространился и на взаимодействия с другими заинтересованными министерствами и ведомствами. В идеале Московский университет, как представляется, мог бы заключить подобные соглашения со всеми министерствами и ведомствами, представленными в Межведомственной комиссии по информационной безопасности Совета Безопасности Российской Федерации.
- Президиум Совета Учебно-методического объединения университетов России от 19 февраля 2001 г. принял решение о создании в объединении секции по гуманитарным проблемам информационной безопасности. Теперь стоит задача создать рабочую группу указанной секции для подготовки и практической реализации ее решений.

Учитывая потребности в высококвалифицированных специалистах по информационной безопасности, необходимо продолжить работу по созданию в МГУ системы образования в данной области. Эта система по сути своей является междисциплинарной, многоуровневой, поэтому при ее создании необходимо обеспечить выполнение следующих принципов:

1. Все виды и формы обучения должны вестись под единым методическим руководством.
2. Необходимо искать заказчиков и создавать условия для развития различных форм обучения, включая:
   - Обучение по специальностям блока 075000;
   - Обучение по новым специализациям внутри имеющихся специальностей (пример — мехмат и ВМиК; предпосылки для открытия новых специализаций есть также на психологическом, социологическом и юридическом факультетах);
   - Обучение по новым военно-учетным специальностям;
   - Платное обучение в магистратуре по информационной безопасности;
   - Различные формы дополнительного образования (курсы повышения квалификации, курсы переподготовки, дополнительная квалификация, второе высшее образование);
   - Включение в учебный процесс различных факультетов блоков знаний по тем или иным аспектам информационной безопасности (с помощью спецкурсов, спецсеминаров, курсовых работ, дополнений к государственным стандартам образования и т. д.)

Как известно, решением от 28 марта 2001 г. секция по информационной безопасности научного совета при Совете Безопасности Российской Федерации одобрила проекты «Основных направлений научных исследований в области информационной безопасности Российской Федерации» и «Приоритетных проблем научных исследований в области информационной безопасности Российской Федерации».

Среди этих направлений научных исследований в области гуманитарных проблем выделены следующие блоки проблем:

1. **Общеметодологические проблемы информационной безопасности (философские, политические, экономические, культурологические).**

1.1. Определение закономерностей развития информационной сферы как системообразующего фактора жизни современного общества.
1.2. Информационная безопасность как междисциплинарная отрасль научного знания, проблемы ее взаимоотношений с другими науками.
1.3. Проблемы взаимоотношений основных концепций информационной безопасности и других наук.
1.4. Разработка путей и способов использования информационной сферы для решения основных социально-политических задач России на современном этапе.
1.5. Разработка и обоснование критериев и методик оценки состояния информационной безопасности.

2. Проблемы развития правового обеспечения информационной безопасности (юридические).

2.1. Проблемы правового регулирования, обеспечения и защиты интересов личности и общества в информационной сфере.
2.2. Проблемы правового регулирования в области информационного обеспечения государственной политики Российской Федерации.
2.3. Проблемы правового обеспечения отечественной индустрии информации и современных информационных технологий.
2.4. Проблемы правового обеспечения безопасности информационных и телекоммуникационных систем.
2.5. Проблемы международно-правового регулирования в области информационной безопасности.

3. Проблемы обеспечения безопасности индивидуального, группового и массового сознания (социологические, психологические).

3.1. Исследование места и роли проблем информационной безопасности в социальных процессах современного российского общества.
3.2. Проблемы информационно-психологической безопасности личности и общества.

Уже сами наименования направлений научных исследований наглядно свидетельствуют о том, что информационная безопасность является новым и очень сложным, многоплановым объектом междисциплинарных гуманитарных научных исследований. Понять природу, механизм его функционирования можно только с привлечением понятийного аппарата и инструментария разных гуманитарных наук — социологии, психологии, права, политологии и др. Причем, особенно важно, чтобы была оптимальная корреляция фундаментальных научных исследований, с одной стороны, и прикладных разработок (мониторинги, опросы, контент-анализы и т. д.), с другой.

Исходя из этого понимания статуса и роли информационной безопасности, данная сфера должна стать темой серьезного и развернутого междисциплинарного научного проекта, поддержанного на государственном уровне. Как представляется, выработанные направления исследований могут быть взяты в качестве ориентиров при подготовке и создании новых специальностей в гуманитарной составляющей информационной безопасности.

В целом, общий принцип подготовки кадров в области информационной безопасности — это подготовка специалистов на базе фундаментального (университетского) образования, поскольку они в первую очередь должны быть специалистами в той или иной области, чтобы затем на базе профессиональных знаний получить дополнительное образование в сфере информационной безопасности.

Поэтому, в частности, особое внимание должно быть уделено развитию магистратуры как формы и этапа обучения в вузах, например, в университете. Специалисты, которые требуются сегодня, должны иметь фундаментальное базовое образование, к которому дополнительно надо дать «надстройку» в виде специализации по информационной безопасности. Например, экономистам необходимо дополнительное образование по специальности «электронная экономика», которую в полном объеме сегодня нельзя получить в рамках существующих экономических специальностей, юристам необходима специализация в сфере правового обеспечения безопасности информационных и телекоммуникационных систем, в частности, в сфере компьютерной преступности, которая набирает темпы по всему миру по мере становления информационного общества. Такие специализации можно

полноценно организовать, как представляется, на базе дополнительного образования (например, магистерского уровня).

Востребованность специалистов в области обеспечения информационной безопасности уже сегодня высока, а по мере вхождения России в информационное общество, без сомнения, будет увеличиваться. Чтобы отвечать требованиям времени, необходимо продолжить развитие этой формы образования.

Первые шаги в направлении развития методологических исследований по проблемам обеспечения информационной безопасности и подготовки специалистов (кандидатов и докторов наук) в области информационной безопасности и предпринимает Московский университет. На очереди — создание в университете докторского диссертационного совета по гуманитарным аспектам проблематики обеспечения информационной безопасности. Этот вопрос уже решен в принципиальном плане Ректором, и теперь необходимо активизировать работу по его практической реализации. Во многих советах страны диссертации по данным проблемам уже защищаются, и хотелось бы, чтобы МГУ и здесь «задавал тон».

Специалистами заинтересованных министерств и ведомств по поручению Совета Безопасности Российской Федерации в настоящее время разрабатывается проект федеральной программы реализации первоочередных мероприятий, предусмотренных Доктриной информационной безопасности Российской Федерации. Задача ученых МГУ, разрабатывающих проблематику информационной безопасности — активно поучаствовать в формировании и реализации данной программы. Одной из форм участия в этой работе может стать проведение конкретных научно-исследовательских работ по заказам федеральных органов, в том числе — исполнительной власти.

Перечень мероприятий, включенных в раздел 9 Доктрины информационной безопасности, дает основание говорить о комплексной межведомственной многоцелевой федеральной программе, которая, по сути своей, должна состоять из нескольких взаимоувязанных подпрограмм. Одной из таких подпрограмм должна быть подпрограмма научных исследований, сформированная на основе перечня приоритетных проблем, который разработала секция по информационной безопасности научного совета при Совете Безопасности Российской Федерации.

Для координации разработки и последующей реализации федеральной программы целесообразно сформировать Совет программы, в который должны войти представители заинтересованных ведомств и учреждений. Совет программы мог бы готовить ежегодный доклад о ходе реализации программы и выбирать (на конкурсной основе) проекты для реализации в рамках Федеральной программы на следующий год.

Важным направлением научной деятельности в области информационной безопасности является также международное научное сотрудничество. Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности на заседании от 26 декабря 2000 г. рассмотрела данный вопрос и отметила, что одним из актуальных направлений реализации Доктрины информационной безопасности Российской Федерации является создание международной системы информационной безопасности. Важным шагом в этом направлении явилось участие специалистов и ученых федеральных органов исполнительной власти в международной научно-практической конференции «Научные проблемы информационной безопасности» 25–27 июня 2001 г. в МГУ им. М. В. Ломоносова, а также образование рабочей группы «Влияние информационных технологий на национальную безопасность» в Консорциуме военных академий и институтов, изучающих проблемы безопасности, стран-участниц программы «Партнерство ради мира».

Из всего изложенного ясно, что проблемы подготовки кадров в области информационной безопасности имеют ярко выраженный междисциплинарный и межведомственный характер. Эти проблемы в их нынешнем, практически нерешенном пока состоянии существенно сдерживают развитие учебного процесса, особенно по гуманитарным направлениям информационной безопасности. Для решения их представляется целесообразным объединить усилия заинтересованных ведомств и создать межведомственный учебно-методический центр по информационной безопасности.

Гуманитарное образование в области информационной безопасности надо всемерно развивать и совершенствовать с целью создания полноценной системы подготовки специалистов в ее «гуманитарном спектре», что соответствовало бы характеру задач, вытекающих из Доктрины информационной безопасности.

Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации

А. А. Стрельцов

К числу важных научно-методологических проблем правового обеспечения информационной безопасности Российской Федераций относится раскрытие его содержания как направления деятельности государства, которое характеризуется целью, структурой и методами [1].

1. Известно, что общая цель права заключается в создании условий для реализации свободы человека, в противодействии произволу и насилию в отношении его как со стороны других людей, общественных организаций, так и государства. Как отметил С. С. Алексеев, «именно право по своей исходной сути представляет собой образование из жизни людей, которое логически и исторически предназначено быть институтом, призванным реализовывать свободу каждого человека, придавать ей определенность и обеспеченность, а отсюда — истинно человеческую ценность» [2].

Произвол и насилие особенно опасны в информационной сфере, т. к. осуществляются в отношении одного из основных условий жизни человека и общества — информации. Произвол и насилие составляют основное содержание угроз безопасности информации, информационной инфраструктуры, правового статуса субъектов информационной сферы, и их проявление сопряжено с нанесением вреда социальным интересам личности, интересам общества или государства.

Противодействие угрозам безопасности объектов национальных интересов в информационной сфере правовыми средствами является основной целью правового обеспечения информационной безопасности, включает ликвидацию угроз и минимизацию ущерба от проявления угроз, достигаемую посредством

предупреждения, пресечения или минимизации последствий проявления этих угроз.

Ликвидация угроз как цель функционирования правового механизма обеспечения информационной безопасности заключается в создании таких условий взаимодействия личности, общества и государства с источниками угроз, при которых это взаимодействие из стадии дисгармонии или конфликта переходит в стадию гармонии. Эта цель достигается посредством оказания правового воздействия, направленного на изменение содержания интересов субъектов, выступающих в качестве либо источника, либо средства реализации угроз, на ликвидацию средств осуществления угроз, имеющихся в их распоряжении, а также на обеспечение неотвратимости претерпевания ими определенного ущемления их интересов в случае обнаружения признаков подготовки к реализации угрозы.

На достижение подобных целей направлена деятельность по обеспечению безопасности международного сообщества и Российской Федерации. Так, для ликвидации угрозы применения Ираком оружия массового поражения, других угроз интересам международного сообщества, ООН создала правовые условия для принуждения Ирака к добровольному разоружению или разоружению в условиях использования для этого международных вооруженных сил. В целях ликвидации угрозы вооруженного разрешения конфликтного взаимодействия с сепаратистским политическим руководством Чеченской Республики, угроз другим национальным интересам в 1996–2000 гг. Российской Федерацией были созданы правовые условия сначала для наведения в Чеченской Республике конституционного порядка с использованием вооруженных сил, затем — для обеспечения независимого, автономного существования Чеченской Республики в рамках Российской Федерации и, наконец, для уничтожения этих вооруженных банд и реализации политического процесса восстановления Чеченской Республики в качестве субъекта Российской Федерации.

Аналогичные цели могут возникать и в отношении правового противодействия угрозам национальным интересам в информационной сфере. Так, ликвидация угрозы монополизации средств массовой информации может достигаться посредством правового запрета некоторым субъектам информационной сферы учреждения средств массовой информации, если при этом нарушаются

принципы добросовестной конкуренции в распространении массовой информации на территории Российской Федерации. Ликвидация угрозы нарушения правового статуса человека и гражданина в информационной сфере со стороны органов государственной власти может достигаться посредством интернационализации процедуры рассмотрения которых конфликтных ситуаций в этой области, при которой соответствующие дела подведомственны как национальным, так и международным судебным органам, обладающим полномочиями применения к виновным должностным лицам установленной юридической ответственности.

В то же время в отношении значительного числа угроз безопасности объектов национальных интересов в информационной сфере постановка цели их ликвидации не всегда представляется возможной, ввиду отсутствия необходимых для ее достижения социальных, политических, экономических и других ресурсов. В этих случаях цель функционирования правовых механизмов противодействия угрозам может заключаться в предупреждении и пресечении проявления этих угроз, а также минимизации последствий их проявления.

Предупреждение проявления угроз заключается в создании условий, при которых вероятность проявления этих угроз существенно снижается. Это достигается в тех случаях, когда существенно снижается ожидаемый от реализации угроз политический, экономический, социальный или иной эффект вследствие либо возможности применения к субъектам, посредством действий которых реализуются угрозы, достаточной меры юридической ответственности, либо повышения защищенности объектов угроз. Так, угроза уничтожения документов, имеющих важное значение для сохранения и развития нации, может быть в существенной степени предупреждена путем установления особого правового режима данных документов, определяющего порядок их хранения и доступа к ним, а также возможности применения достаточной меры юридической ответственности к лицам, виновно нарушающим этот режим.

Пресечение проявления угроз направлено на выявление фактов проявления угроз и принятие мер по прекращению негативного воздействия на объект национальных интересов в информационной сфере. Так, пресечение проявления угрозы осуществления компьютерных преступлений как цель правового обеспечения информационной безопасности заключается в создании условий,

при которых надежно и оперативно может быть установлен факт начала противоправного деяния, субъект этого деяния, зафиксированы в требуемой для представления в судебные органы форме признаки объективной и субъективной составляющих преступления и приняты меры для прекращения противоправного деяния.

Минимизация последствий проявления угроз заключается в создании правовых условий для уменьшения причиняемого ущерба, а также для ликвидации, если это возможно, последствий проявления угроз. Это может быть достигнуто путем правового закрепления требований к защищенности данных объектов, а также установления порядка возмещения субъектами, причинившими ущерб, средств, затраченных на ликвидацию последствий проявления угроз. Так, минимизация последствий проявления угроз безопасности функционирования критически важных объектов национальной информационной инфраструктуры может быть достигнута правовым закреплением регламентов, устанавливающих требования по сертификации технического и программного обеспечения этих объектов, организации системы управления безопасностью, а также процедуры контроля уровня их реальной защищенности и ответственности должностных лиц за соблюдение регламентов и предписаний контролирующих органов.

Определение целей правового обеспечения информационной безопасности осуществляется на основе анализа характеристик объектов безопасности и угроз, а также возможности оказания эффективного правового воздействия на общественные отношения, посредством которых угрозы проявляются.

2. В структуре правового обеспечения информационной безопасности как вида деятельности выделяются:

- нормативное правовое обеспечение информационной безопасности;
- правовое обеспечение информационной безопасности как направление юридической науки;
- правовое обеспечение информационной безопасности как система учебных курсов, используемых в процессе подготовки кадров для деятельности в области противодействия угрозам информационной безопасности.

2.1. Нормативное правовое обеспечение информационной безопасности. Механизмы правового регулирования

отношений в области противодействия угрозам безопасности объектов национальных интересов в информационной сфере реализуются посредством нормативного правового обеспечения информационной безопасности и правоприменительной практики, осуществляемой уполномоченными органами исполнительной власти. Нормативное правовое обеспечение образуется совокупностью правовых институтов и норм, регулирующих отношения, связанные с проявлением угроз нанесения вреда объектам национальных интересов в информационной сфере и, как следствие, с ущемлением социальных интересов личности, общества и государства. Оно определяет «потенциальную» эффективность правового регулирования в этой области, т. е. способность создать субъектам ее обеспечения необходимые условия для недопущения нанесения вреда объектам национальных интересов в информационной сфере. С этой точки зрения нормативное правовое обеспечение может рассматриваться как «идеальное» правовое обеспечение.

В зависимости от объекта обеспечения информационной безопасности в составе нормативного правового обеспечения выделяются четыре составляющих:

- нормативное правовое обеспечение безопасности информации в форме сведений;
- нормативное правовое обеспечение безопасности информации в форме сообщений;
- нормативное правовое обеспечение безопасности информационной инфраструктуры общества;
- нормативное правовое обеспечение безопасности правового статуса субъектов информационной сферы.

Нормативное правовое обеспечение безопасности информации в форме сведений образуется совокупностью правовых институтов и норм, регулирующих отношения в области противодействия угрозам нанесения вреда свободе психической деятельности человека и субъективной значимости национальных культурных ценностей.

Нормативное правовое обеспечение безопасности информации в форме сообщений образуется совокупностью правовых институтов и норм, регулирующих отношения в области противодействия угрозам сохранности сообщений, являющихся важными для сохранения и развития нации как социальной общности. К их

числу относятся, например, документы, хранящиеся в Фонде документов, составляющих культурную ценность Российской Федерации, включая документы Архивного фонда Российской Федерации, Музейного фонда Российской Федерации и библиотечного фонда.

Нормативное правовое обеспечение безопасности информационной инфраструктуры образуется совокупностью правовых институтов и норм, регулирующих отношения в области противодействия угрозам нарушения работоспособности и функционирования основных составляющих этой инфраструктуры — информационных и телекоммуникационных систем, сетей связи, системы массовой информации и т. п.

Нормативное правовое обеспечение безопасности правового статуса субъектов в информационной сфере образуется совокупностью правовых институтов и норм, регулирующих отношения в области противодействия угрозам ущемления прав человека и гражданина, организаций и учреждений, органов государственной власти на осуществление информационной деятельности, неисполнения им возложенных обязанностей в области этой деятельности и, как следствие, нанесения ущерба деятельности по реализации социальных интересов личности, интересов общества и государства.

Нормативное правовое обеспечение информационной безопасности закрепляется в системе нормативных правовых актов, выступающих в качестве источников права и образующих его внешнюю форму [3]. К числу таких источников права относятся Конституция Российской Федерации, международные договоры Российской Федерации, федеральные законы, нормативные правовые акты Президента Российской Федерации, подзаконные акты Правительства Российской Федерации, а также нормативные правовые акты законодательной и исполнительной властей субъектов Российской Федерации, принятые по вопросам, отнесенным к их компетенции. Кроме того, к источникам права в этой области относятся решения Конституционного Суда Российской Федерации, а также разъяснения Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации. При рассмотрении нормативного правового обеспечения информационной безопасности представляется важным определить его место в системе объективного права и системе законодательства.

В системе объективного права, по мнению специалистов, нормативное правовое обеспечение информационной безопасности является одной из составляющих информационного права. Так, В. Н. Лопатин полагает, что «поскольку отношения, возникающие в связи с обеспечением информационной безопасности, относятся как к информационной сфере, так и к сфере обеспечения национальной безопасности, можно считать, что право в области обеспечения информационной безопасности — это подотрасль информационного права, представляющая собой совокупность правовых норм, регулирующих общественные отношения по защите национальных интересов в информационной сфере (жизненно важных интересов личности, общества и государства на сбалансированной основе) от угроз» [4]. Близкую позицию занимает В. А. Копылов, который рассматривает нормативное правовое обеспечение информационной безопасности в качестве отдельной составляющей информационного права и выделяет в ней «три основных направления правовой защиты объектов в информационной сфере: защиту чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности, нравственных и эстетических идеалов, стабильности и устойчивости развития общества, информационного суверенитета и целостности государства; защиту информации и информационных ресурсов, а также информационных систем, информационных технологий, средств связи и телекоммуникаций; защиту информационных прав и свобод личности» [5].

В системе законодательства нормативное правовое обеспечение информационной безопасности рассматривают в качестве составляющей информационного законодательства. Так, И. Л. Бачило, формулируя перечень условно выделенных блоков проблем информационного законодательства, включает в него информационную безопасность и полагает, что она «аккумулирует проблемы защиты открытой информации, охраны государственной тайны, обеспечения защиты информации ограниченного доступа, кроме государственной тайны, страхование информации, информационных ресурсов, а также реализует все направления правового регулирования в соответствии с доктриной информационной безопасности личности, общества и государства» [6]. Т. А. Полякова полагает, что нормативное правовое обеспечение информационной безопасности является подразделом информационного законодательства [7].

По мнению автора, такое определение места нормативного правового обеспечения информационной безопасности в системе права и системе законодательства не вполне обосновано.

С одной стороны, нормативное правовое обеспечение информационной безопасности в целом ряде случаев, безусловно, развивает механизмы правового регулирования отношений, составляющих предмет информационного права, который, как было показано ранее [8], образуется совокупностью общественных отношений, возникающих в процессе взаимодействия с целью удовлетворения интересов субъектов в обладании необходимой информацией, в передаче части имеющейся информации другим субъектам, в сохранении оставшейся части информации неизвестной им. Наличие особого предмета правового регулирования, по мнению специалистов [9], выделяет информационное право в самостоятельную комплексную отрасль права, в которой не формируется самостоятельный метод правового регулирования в полном смысле этого слова. В ней аккумулируются все методы правового воздействия, используемые в пределах ее предмета. Ряд институтов и норм, составляющих основное содержание нормативного правового обеспечения информационной безопасности, направлены на регулирование «информационных» отношений, и, видимо, могут рассматриваться в качестве элементов информационного права, а закрепляющие их нормативные правовые акты — в качестве составляющих информационного законодательства.

С другой стороны, ряд норм, образующих нормативное правовое обеспечение информационной безопасности, развивает правовые механизмы, регулирующие общественные отношения, относящиеся к другим отраслям права, в том числе таких базовых отраслей как конституционное, гражданское, административное и уголовное право [10]. Отнесение этих норм к информационному праву отрывает их от родовых отраслей, чем создает сложности для развития, прежде всего, самого информационного права, поскольку включает в его предмет отношения, не являющиеся «информационными».

В связи с этим представляется целесообразным рассматривать правовое обеспечение информационной безопасности в качестве самостоятельного комплексного направления правового регулирования, осуществляемого в рамках реализации государственной политики в области обеспечения информационной безопасности. Оно образуется совокупностью институтов и норм

информационного, конституционного, гражданского, административного и уголовного права, регулирующих отношения в области противодействия угрозам безопасности объектов национальных интересов в информационной сфере.

Возможно, что в перспективе оно станет составляющей еще не сформировавшегося права обеспечения национальной безопасности и соответствующего законодательства.

2.2. Научная составляющая правового обеспечения информационной безопасности. Важной составной частью структуры правового обеспечения информационной безопасности являются научные исследования отношений, составляющих его предмет, изучение правовой характеристики объектов национальных интересов в информационной сфере, способов проявления угроз этим объектам, правовых средств и механизмов, способных обеспечить противодействие угрозам, способов взаимодействия различных отраслей права в процессе функционирования механизмов правового регулирования отношений в данной предметной области, а также проведение сравнительных исследований методов правового регулирования аналогичных отношений в различных странах мира, вопросов взаимодействия национального права и международного права.

Эта часть правового обеспечения информационной безопасности развивалась преимущественно на основе публикаций периодических изданий, частично на монографических исследованиях и разработках курсов учебной литературы. Среди наиболее значимых работ следует назвать труды Ю. М. Батурина, И. Л. Бачило, В. Н. Лопатина, А. А. Фатьянова, В. А. Копылова, М. М. Рассолова, А. В. Морозова, Т. А. Поляковой, П. У. Кузнецова, М. А. Вуса, С. И. Семилетова и некоторых других.

В то же время развитие теории правового обеспечения информационной безопасности находится в начальной стадии и для его становления в качестве самостоятельной области научного исследования требуется проведение значительного объекта исследований. В связи с тем, что информационное право как научная дисциплина тоже находится в начале своего развития, эти исследования должны быть направлены как на изучение закономерностей использования правовых средств для регулирования отношений, связанных с информацией и составляющих предмет научных исследований в области информационного права, так

и на изучение закономерностей использования правовых средств для противодействия угрозам безопасности национальных интересов в информационной сфере.

К числу актуальных научных задач правового обеспечения информационной безопасности относятся следующие.

Во-первых, разработка методов анализа правовых условий, способствующих проявлению угроз безопасности основным объектам национальных интересов в информационной сфере. Этот анализ предполагает изучение условий проявления угроз, механизмов правового регулирования отношений, связанных с этими объектами, выявление пробелов и противоречий в правовых нормах, а также причин недостаточной в ряде случаев эффективности правового регулирования отношений в рассматриваемой области.

Во-вторых, разработка методов конструирования эффективных правовых механизмов противодействия угрозам, обеспечивающих предупреждение их проявления, выявление фактов проявления угроз, пресечение действий, опосредующих угрозы, и ликвидацию последствий проявления угроз. В частности, представляется важной разработка методов повышения активности использования субъектами дозволений, отражающих меру предоставленной им свободы поведения, возможность требования исполнения корреспондирующих обязанностей и реализации притязаний, определения достаточной степени юридической ответственности, применяемой к лицам, нарушающим правовые установления и вследствие этого наносящим ущерб объектам национальных интересов в информационной сфере, обеспечения надлежащего исполнения возложенных на них обязанностей и т. п. Решение этой проблемы связано с определением системы правовых средств, способных оказать необходимое воздействие на субъектов регулируемых общественных отношений. Оно должно побудить их к участию в правоотношениях, возникающих в связи с существованием соответствующих правовых установлений, либо к активизации правоприменительной практики, связанной с реализацией правоотношений, возникающих вследствие возникновения условий или событий, предусмотренных установлениями.

В-третьих, разработка методов оценки эффективности правового обеспечения информационной безопасности, позволяющих установить реальную степень воздействия права на субъектов реализации угроз безопасности объектов национальных интересов в информационной сфере.

Научные знания в области правового обеспечения информационной безопасности позволяют, с одной стороны, повысить эффективность правового регулирования отношений в рассматриваемой области, а с другой — создать условия для подготовки кадров для субъектов обеспечения информационной безопасности.

2.3. Учебные дисциплины по правовому обеспечению информационной безопасности. Третьей составной частью правового обеспечения информационной безопасности являются результаты обобщения исследований и анализа законодательства по выделенным выше составляющим нормативного правового обеспечения и постановка на этой основе курсов учебных дисциплин.

Эти учебные курсы должны быть ориентированы на подготовку специалистов различного уровня подготовки и профиля специализации. По уровню подготовки различаются учебные курсы для лиц, получающих базовое образование, и для лиц, повышающих свою квалификацию (получающих дополнительное образование) или меняющих ее и уже обладающих тем или иным базовым высшим образованием. По профилю специализации различают учебные курсы для специалистов в области конституционного, информационного, гражданского, административного и уголовного права, которые должны знать механизмы правового противодействия угрозам безопасности объектов национальных интересов в информационной сфере, связанных с регулируемыми ими общественными отношениями.

3. Как было отмечено выше, в структуре правового обеспечения информационной безопасности выделяются три основные составляющие: нормативное правовое обеспечение, научные исследования и учебные курсы. В основе каждой из этих составляющих лежат ключевые положения, определяющие их построение и функционирование, называемые принципами, и каждая из этих составляющих использует для решения стоящих перед ней задач определенные методы.

3.1. Принципы и методы нормативного правового обеспечения информационной безопасности. Принципы нормативного правового обеспечения информационной безопасности определяют общую основу составляющих его правовых институтов и норм, а методы — приемы юридического воздействия

на соответствующие общественные отношения, их сочетание, характеризующие использование того или иного комплекса юридических средств. К принципам нормативного правового обеспечения информационной безопасности следует отнести: законность, целенаправленность, дополнительность, адекватность, полноту и непротиворечивость.

Принцип законности заключается в обеспечении соответствия правовых норм, составляющих правовое обеспечение информационной безопасности, Конституции Российской Федерации, общепринятым принципам и нормам международного права, международным договорам Российской федерации, федеральному законодательству.

Принцип целенаправленности заключается в использовании правовых средств, позволяющих достичь преследуемых государством целей противодействия угрозам безопасности объектов национальных интересов в информационной сфере.

Принцип дополнительности заключается в развитии механизмов правового регулирования общественных отношений, связанных с объектами национальных интересов в информационной сфере, посредством дополнения этих механизмов нормами, призванными противодействовать проявлению угроз безопасности данных объектов.

Принцип адекватности заключается в соответствии правовых средств воздействия на общественные отношения, посредством которых проявляются угрозы, социальной опасности этих угроз.

Принцип полноты заключается в охвате правовым регулированием всех наиболее важных общественных отношений, связанных с проявлением угроз безопасности и противодействием этим угрозам.

Принцип непротиворечивости заключается в согласованности правовых норм, регулирующих общественные отношения в рассматриваемой области, в отсутствии в этих нормах пробелов и противоречий.

Методы нормативного правового обеспечения информационной безопасности представляют собой способы использования правовых средств для противодействия угрозам безопасности объектов национальных интересов в информационной сфере. Они базируются на исходных, первичных методах, представляющих собой простейшие приемы регулирования: методе централизованного регулирования (субординации), при котором в основе

регулирования лежат властно-императивные начала, предписывающие участникам отношений необходимость осуществления некоторых действий, и методе децентрализованного регулирования (координации), при котором источником правовой активности являются сами субъекты отношений [11].

Эти методы создают основу отраслевых методов, выражающих особые юридические режимы регулирования. К ним в области нормативного правового обеспечения информационной безопасности относятся методы правового режима объекта безопасности, запрета, юридической ответственности, позитивного обязывания и некоторые другие.

В целях стимулирования деятельности по реализации и применению права (т. е. активного использования субъектами своих прав и выполнения обязанностей, включая право требования и притязания, активной правоприменительной практики со стороны органов исполнительной власти, которая, в свою очередь, предполагает заинтересованность субъектов информационной сферы и должностных лиц в осуществлении этой деятельности) в правовом обеспечении информационной безопасности используются методы поощрения, убеждения и принуждения.

3.2. Принципы и методы правового обеспечения информационной безопасности как направления юридической науки. Принципы правового обеспечения информационной безопасности как направления юридической науки представляют собой совокупность основных положений, обеспечивающих получение достоверных научных знаний о предмете исследования, о закономерностях использования правовых средств противодействия угрозам безопасности объектов национальных интересов в информационной сфере, формах и методах правового противодействия угрозам. К числу таких принципов относятся общие принципы юридической науки [12]:

- историзм, заключающийся в необходимости «изучения не только последовательно и неумолимо повторяющихся событий и процессов в истории права, но и правовых явлений единичных и тем не менее именно в силу своей единичности, а не универсальности, очень важных для понимания и определения права» [13] вообще и правового обеспечения информационной безопасности, в частности;

- системность, означающий необходимость взаимосвязанного рассмотрения всех составляющих правового обеспечения информационной безопасности, выявления основных ее структурных составляющих, элементов, анализа существующих между ними отношений, а также их взаимосвязи с реальными общественными отношениями;
- объективность, означающий независимость научных выводов и положений от конъюнктуры и политической ангажированности.

Методы правового обеспечения информационной безопасности как направления юридической науки представляют собой способы, с помощью которых изучаются возникновение, функционирование и развитие правовых механизмов регулирования отношений в области противодействия угрозам безопасности объектам национальных интересов в информационной сфере. Они образуются совокупностью общенаучных методов, используемых в общественных науках, общих теоретико-правовых методов и специфических методов исследования нормативного правового обеспечения информационной безопасности. К общенаучным методам относятся, например: диалектический метод, заключающийся в рассмотрении предмета исследования с точки зрения основных законов диалектического знания (перехода количества в качество, единства и борьбы противоположностей, отрицания отрицания); исторический метод, заключающийся в учете при исследовании динамики изменения предмета на некотором достаточно длительном интервале времени; системный метод, заключающийся в исследовании предмета как целостной, упорядоченной совокупности компонентов, взаимодействие которых порождает новое, не присущее им качество; некоторые другие методы. К теоретико-правовым методам относятся: формально-логический, заключающийся в логическом анализе внутреннего строения правовых норм и институтов, отраслей права, его источников и позволяющий на этой основе осуществлять классификацию и систематизацию явлений правовой действительности, проводить исследование внешней и внутренней форм права; сравнительный метод, заключающийся в исследовании правовых механизмов, применяемых для регулирования однородных общественных отношений в различных, национальных системах права; метод изучения эффективности действия правовых норм,

заключающийся в использовании социологических и статистических исследований правового поведения субъектов, и некоторые другие.

Специфические методы исследования правового обеспечения информационной безопасности включают методы:

- толкования государственной политики в этой области;
- систематизации правовых механизмов регулирования отношений в области проявления угроз безопасности объектов национальных интересов в информационной сфере и противодействия этим угрозам, а также систематизации законодательства, закрепляющего данные правовые механизмы;
- анализа правовых норм, реализующих правовые механизмы регулирования отношений в области проявления угроз безопасности объектов национальных интересов в информационной сфере и противодействия этим угрозам;
- определения приоритетных направлений совершенствования правовых механизмов и соответствующих правовых норм.

Методы толкования государственной политики в области обеспечения информационной безопасности призваны обеспечить, исходя из содержания политических и иных документов, определяющих основное содержание национальных интересов в информационной сфере и угроз безопасности этих интересов, обоснованное отграничение предметной области и цели правового обеспечения. Толкование государственной политики как и толкование права включает два основных элемента [14]: уяснение, т. е. раскрытие «для себя» содержания задач деятельности государства в рассматриваемой области, выбранных принципов и методов их выполнения, определение роли и места правового регулирования в этом процессе, и разъяснение, т. е. раскрытие целей и направлений правового обеспечения «для других».

Методы систематизации правовых механизмов регулирования отношений в области проявления угроз безопасности объектов национальных интересов в информационной сфере и противодействия им позволяют упорядочить совокупность используемых для этого правовых методов и средств.

Методы анализа правовых норм, закрепляющих рассматриваемые правовые механизмы, направлены на выяснение полноты

охвата регулированием предметной области правового обеспечения и степени совершенства юридической техники нормативного закрепления юридических конструкций, используемых для противодействия угрозам безопасности объектов национальных интересов в информационной сфере.

Методы определения приоритетных направлений совершенствования правовых механизмов и соответствующих правовых норм позволяют выявить условия наиболее опасного проявления угроз, а также сформировать правовые конструкции, позволяющие обеспечить достижение целей правового обеспечения применительно к этим условиям, и закрепляющие их правовые нормы.

Выбор методов определяется целями и задачами научного исследования, общим уровнем научного знания в конкретной области, его возможностями, но, прежде всего, особенностями самого предмета научного исследования.

Система общенаучных методов, общих теоретико-правовых методов и специфических методов исследования средств правового регулирования отношений, возникающих вследствие проявления угроз безопасности объектов национальных интересов в информационной сфере, образует методологию правового обеспечения информационной безопасности.

Исследования правового обеспечения включают следующие основные этапы:

- анализ правовых характеристик объекта национальных интересов в информационной сфере, в рамках которого выясняются вопросы правового закрепления объекта отношений, основные группы связанных с ним общественных отношений и механизмы их правового регулирования;
- анализ содержания угрозы безопасности объектов национальных интересов, в рамках которого выясняются основные способы нанесения вреда этим объектам вследствие проявления угроз;
- анализ правового обеспечения безопасности объектов, в рамках которого выясняется его предмет, а также цели, принципы и методы правового регулирования общественных отношений, составляющих данный предмет, закрепляющие их правовое нормы, их достаточность для эффективного противодействия угрозам безопасности объектов национальных интересов;

- разработка предложений по совершенствованию правового обеспечения информационной безопасности, в рамках которой подготавливаются предложения по развитию правовых норм и механизмов, регулирующих отношения, возникающие вследствие проявления угроз безопасности объектам национальных интересов в информационной сфере, в целях повышения защищенности этих объектов.

Каждый из этих этапов предполагает использование своих методов исследования. Так, анализ правовых характеристик объекта национальных интересов в информационной сфере осуществляется с использованием метода дедукции, формально-логического метода и методов толкования норм права, анализ содержания угроз безопасности объектов национальных интересов осуществляется с использованием методов системного анализа, сравнительно-правового анализа и логического моделирования, анализ правового обеспечения безопасности объектов национальных интересов в информационной сфере осуществляется с использованием методов системного анализа и структурного моделирования, а разработка предложений по совершенствованию правовых механизмов противодействия угрозам — с использованием диалектического метода, метода системного анализа и формально-логического метода.

3.3. Принципы и методы правового обеспечения информационной безопасности как совокупности учебных курсов. Принципы правового обеспечения информационной безопасности как совокупности учебных курсов представляют собой совокупность основных положений, отражающих общий подход к развитию этого сектора системы образования. К числу таких принципов относятся:

- подготовка специалистов по правовому обеспечению информационной безопасности на базе фундаментального юридического и достаточного технического образования при углубленном изучении основ тех отраслей права, которые являются для него базовыми: конституционного, гражданского, административного, информационного и уголовного права;
- изучение в рамках учебных курсах основ философии, социологии, психологии, культурологии, политологии и информатики в объеме, достаточном для понимания роли

и места информации, информационной инфраструктуры в жизни человека и общества, в реализации государственного управления, форм существования информации и особенностей ее обращения в обществе.

Методы правового обеспечения информационной безопасности как системы учебных курсов образуются совокупностью методов обучения учащихся, привития им навыков и оказания помощи в овладении знаниями, необходимыми для удовлетворения требованиям, предъявляемым к специалистам соответствующих специальностей.

Таким образом, *правовое обеспечение информационной безопасности как вид деятельности направлено на противодействие угрозам безопасности основных объектов национальных интересов в информационной сфере. Структурно оно включает самостоятельное направление правового регулирования, самостоятельную область юридической науки и систему учебных курсов. Каждая из выделенных составляющих правового обеспечения информационной безопасности базируется на определенной системе принципов и использует для решения стоящих перед ней задач свойственную ей систему методов.*

Литература

[1] *Глебов А. П.* Сущностно-субстанциональный и функциональные подходы в исследовании государственных и правовых явлений. В кн.: Проблемы теории государства и права. Под ред. М. Н. Марченко. МГУ им. М. В. Ломоносова, юридический факультет. М.: «Проспект», 1999. С. 145.

[2] *Алексеев С. С.* Право: азбука — теория — философия: Опыт комплексного исследования. М.: «Статут», 1999. С. 250.

[3] Там же. С. 235

[4] *Лопатин В. Н.* Правовые основы информационной безопасности // Информационное право. С. 473.

[5] *Копылов В. А.* Информационное право. С. 219.

[6] *Бачило И. Л.* Информационное право. С. 27.

[7] *Полякова Т. А.* Теоретико-правовой анализ законодательства в области обеспечения информационной безопасности

Российской Федерации. Дисс. ... канд. юридич. наук. Российская правовая академия при Министерстве юстиции Российской Федерации. М., 2002.

[8] *Стрельцов А. А.* Предмет правового обеспечения информационной безопасности. Российский юридический журнал. 2003. № 2.

[9] *Венгеров А. Б.* Теория государства и права. М. 1999. С. 381; *Бачило И. Л.* Информационное право. Основы практической информатики. М. 2001. С. 54.

[10] *Алексеев С. С.* Право: азбука — теория — философия: Опыт комплексного исследования. М.: «Статут», 1999. С. 46.

[11] Там же. С. 371.

[12] *Венгеров А. Б.* Теория государства и права. С. 265.

[13] Там же. С. 231.

[14] *Алексеев С. С.* Государство и право. М.: Юридическая литература, 1994. С. 165.

Информационная безопасность и компьютерный терроризм

В. А. Васенин

Введение

При современном уровне развития высоких технологий расширяются возможности их использования для совершения террористических действий. Во многих странах сегодня ведется активная работа по анализу потенциальных возможностей подобных проявлений и выработке мер по борьбе с этим злом.

О понимании значимости, внимании к этой проблеме и попытках выработки такой системы мер на концептуально-теоретическом и практическом уровнях свидетельствуют, например, неоднократные обсуждения вопросов экстремизма на сетевой среде на межведомственном, междисциплинарном семинаре по научным проблемам информационной безопасности, проводимом в Московском университете под эгидой Совета Безопасности РФ и МГУ, доклады на российско-американском семинаре «Высокотехнологичный терроризм» [1], прошедшем Москве в июне 2001 года, а затем, его продолжении в декабре того же года в США, проводившемся Российской академией наук совместно с Национальными академиями США. На этом семинаре (еще до трагических событий сентября 2001 г.) рассматривались потенциально возможные направления использования различных технологий в террористических целях, включая химическое и бактериологическое, ядерное и компьютерное (кибертерроризм), возможные сценарии их использования, а также системы мер, как стратегического, так и оперативно-тактического характера по противодействию этим угрозам.

Однако, и это следует отметить, многие из обсуждавшихся тогда предложений и сценариев не представлялись столь актуальными. После чудовищных по своему цинизму, масштабам и последствиям актов, совершенных 11 сентября 2001 года

в Нью-Йорке и Вашингтоне, отношение мирового сообщества к этим проблемам стало более острым, а действия — более осознанными, скоординированными и последовательными. В последующие два года обсуждение вопросов терроризма вообще, и высокотехнологического терроризма в частности, проводились на различных форумах национального и международного масштабов, на всех уровнях представительства, — от консультаций специалистов в отдельных относительно «узких» областях до совещаний на уровне глав государств. Подписанные в ходе этих обсуждений документы создают благоприятные условия для активных действий, направленных на противодействие терроризму.

Одним из направлений, по которому на упомянутом российско-американском семинаре с российской стороны выступал автор настоящей публикации [2], был Кибертерроризм (кибернетический или компьютерный терроризм). Глобальное киберпространство и составляющая его основу сеть Интернет рассматривались при этом, как потенциально благоприятное поле для террористической деятельности. Уместно отметить, что компьютерный терроризм и соответствующая ему деятельность по целям и сути своей имеют смысл именно в рамках использования для этого крупной сетевой инфраструктуры или контроля над распределенными в сети важными информационными ресурсами. Данное обстоятельство указывает на типы сетевых объектов и инфраструктуры, которые следует рассматривать в качестве первоочередных объектов атаки террористов на Киберпространстве.

Несмотря на пристальное внимание к отмеченным выше вопросам (которые далее для краткости будет именовать «кибертерроризм» или «компьютерный терроризм»), на наличие документов международного и национального уровня, указывающих на необходимость активных действий на данном направлении, реальных, опубликованных в доступной научно-технической литературе результатов исследований или разработок автору обнаружить не удалось. С одной стороны, это можно объяснить объемным и комплексным характером проблемы в целом, сложной организацией самих объектов первостепенного внимания на сетевой среде и отсутствием должным образом отработанных методологических подходов к анализу, управлению ими и защите. С другой стороны, это еще одно свидетельство недостаточного уровня понимания значимости и восприятия актуальности

проблемы, отсутствия необходимых для начала таких работ побудительных мотивов, в том числе со стороны (а это национальная проблема) государственных ведомств.

С учетом этих обстоятельств, отталкиваясь от основных положений, изложенных в [2], попробуем в данной работе кратко изложить основные концептуальные аспекты модели атаки (явления, феномена), проявления которой можно трактовать как кибертерроризм, а также предложить модель защиты (противодействия), как систему мер для предупреждения или пресечения подобных действий.

Общие положения

Кратко сформулируем основные (отправные, начальные) положения для формирования искомых моделей и системы мер, изложенных в [2].

Терроризм — совокупность противоправных действий, связанных с покушениями на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимуществ при решении политических, экономических или социальных проблем.

Направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов могут быть следующие.

1. Разрушение инфраструктуры сети корпоративного, национального или транснационального масштаба посредством вывода из строя системы управления ею или отдельных подсистем.
2. Несанкционированный (неправомерный) доступ к сетевой информации, охраняемой законом и носящей высокий уровень секретности, нарушение ее целостности, конструктивной управляемости и защищенности.

Следует отличать террористические действия от действий террористов с использованием сетевых ресурсов (в том числе собственных в Интернет) в целях пропаганды своих взглядов, нагнетания обстановки страха, напряженности и т. д.

Ущерб от террористических действий на сетевой среде связан:

- с человеческими жертвами или материальными потерями, вызванными деструктивным использованием элементов сетевой инфраструктуры;
- с возможными потерями (в том числе гибелью людей) от несанкционированного использования информации с высоким уровнем секретности или сетевой инфраструктуры управления в жизненно важных (критических) для государства сферах деятельности;
- с затратами на восстановление управляемости сети, вызванными действиями по ее разрушению или повреждению;
- с моральным ущербом как владельца сетевой инфраструктуры, так и собственного информационного ресурса;
- с другими возможными потерями от несанкционированного использования информации с высоким уровнем секретности.

С учетом изложенных выше положений, анализа моделей нарушителя и моделей атак, рассматриваемых при разработке политик безопасности, при использовании критериальных подходов к оценке уровня защищенности других (в том числе традиционных) компьютерных комплексов, а также моделей гарантированно защищенных систем, в качестве исходной посылки к формированию модели противодействия кибертеррористическим действиям можно рассматривать следующую.

Направления действий на сетевой среде с целью использования их результатов для проведения террористических актов, как набор приемов и методов, представляют собой злоумышленные действия, традиционно рассматриваемые в моделях нарушителя и моделях атак. Такие модели являются необходимым условием для формирования политики информационной безопасности, разработки мер и средств ее реализации в любых ведомственных или корпоративных сетях.

Отличие подходов к предотвращению и реагированию на действия в случае террористического характера целей от других противоправных действий в сетях общего пользования связано с более высоким уровнем требований к безопасности систем, обусловленных их назначением, целями и средой безопасности, и, соответственно, величиной издержек от подобных злоумышленных действий.

О величине убытков от успешных атак на национально значимые сферы хозяйственного комплекса можно судить, например, по результатам инцидентов в 2003 году, связанных с перебоями в электроснабжении крупных регионов США и Канады или нарушениями в системе авиаперевозок в Англии. Потери измерялись сотнями миллионов долларов, а уровень социальной напряженности влиял на политическую обстановку в странах.

В качестве понятия, интегрирующего противодействия кибертерроризму, рассмотрим антитеррористическую информационную безопасность с тем, чтобы подчеркнуть отличие от традиционной информационной безопасности.

Антитеррористическая информационная безопасность — совокупность механизмов, инструментальных средств, методов, мер и мероприятий, позволяющих предотвратить, обнаружить, а в случае обнаружения, — оперативно реагировать на действия, способные привести:

- к разрушению инфраструктуры сети посредством вывода из строя системы управления ею или отдельных ее элементов;
- к несанкционированному доступу к информации, охраняемой законом и носящей высокий уровень секретности, нарушению ее целостности, конструктивной управляемости и защищенности.

Основа антитеррористических действий с использованием сетевой среды — традиционная информационная безопасность, ее методология, модели, механизмы и инструментальные средства. Разработка, построение и сопровождение систем информационной безопасности для отдельных продуктов, изделий и комплексов на сетевой среде, особенно на сетях пакетной коммутации и Интернет, — сложная, многоплановая задача. Её решения строятся с помощью конкретной системы мер, способов и механизмов их реализации на разных уровнях иерархии этой деятельности:

- законодательном;
- операционном;
- административном;
- программно-техническом.

Есть, и это отмечалось в [3], проблемы, связанные с реализацией конкретных мер, механизмов или инструментальных средств на каждом из перечисленных уровней. Степень разрешения этих проблем различна в различных странах и определяется разными факторами (научно-техническая база, уровень

развития сетевой инфраструктуры и т. п.), однако следует отметить, что в «среднем» проблемная область, общая методология информационной безопасности достаточно хорошо проработана и апробирована на традиционных комплексах. Существует, хотя и с разной степенью (и успехом) реализации на практике, необходимая законодательная база.

Вместе с тем, интегрированные распределенные системы информационно-вычислительных ресурсов, используемые для управления национально значимыми сферами хозяйственной деятельности (ведомственные или корпоративные), которые должны быть объектами первостепенного внимания с позиции разработки антитеррористических мер, по целому ряду причин более сложны для анализа и эффективного применения таких мер, чем системы, на которых меры информационной безопасности уже хорошо отработаны и апробированы.

Одной из причин является их сложная внутренняя структура, объективно различные требования, в том числе, по безопасности на отдельные элементы и ресурсы, трудности декомпозиции решений и средств их интеграции. Отмеченные обстоятельства очень затрудняют четкую формулировку политики безопасности для системы в целом и, как следствие, выбор и разработку адекватных средств ее реализации.

Оценка эффективности средств защиты, выполнения ими политики безопасности, обеспечивается либо на основе критериальных подходов [4–20], либо с помощью средств их тестирования, надежной верификации или доказательства гарантированной защищенности для модели системы [21].

Для систем, потенциально уязвимых для кибертеррористических угроз, использование способов второго подхода затруднено и, это отмечалось выше, сложностью построения математических моделей, адекватно отражающих свойства исходной системы, и трудностями их анализа. Столь же сложен для использования критериальный подход к оценке подобных систем на всех этапах её жизненного цикла. Однако, в отличии от аналогичных по сложности комплексов другого назначения, в силу изложенных выше обстоятельств, связанных с высокими требованиями к безопасности рассматриваемых систем, представляется целесообразным при оценке эффективности средств их защиты критериальный подход использовать в обязательном порядке, дополняя его, если это представляется возможным, способами

тестирования, верификации и (или) формирования строгой доказательной базы.

Способы и механизмы операционного и программно-технического уровней на всех этапах жизненного цикла продукта или системы информационных технологий регламентируются требованиями, критериями и показателями информационной безопасности такого объекта оценки. Подобные показатели систематизированы государственными стандартами разных стран от «Оранжевой книги» до ее интерпретации для сетевых конфигураций в США [4–7], «Канадские критерии оценки безопасности информационных технологий» [10], Руководящие документы Гостехкомиссии в России [12–16]). Более того, на этом направлении наблюдается явная, и правильная, по сути, тенденция к международной унификации этих стандартов (Гармонизированные европейские критерии [9] и Общие Критерии ИСО/МЭК 15408 [17–19]). На пути практического применения этих стандартов исследовательские коллективы многих стран активно работают над совершенствованием отдельных механизмов, позволяющих эффективно применять требования к системам информационной безопасности на разных уровнях. Например, в области законодательной — разумный баланс между конфиденциальностью персональной информации и широким доступом к данным общего доступа или международная унификация законодательных актов. В области программно-технической — механизмы ядра ОС для эффективной реализации основных (базовых) сервисов безопасности.

Исходные положения к разработке модели атаки

Принимая как постулат утверждение о том, что традиционная информационная безопасность является основой антитеррористической информационной безопасности, следует отметить, что деятельность по предупреждению и пресечению терроризма на сетевой среде вообще и, особенно в Интернет, имеет свою специфику. Факторы, характеризующие ее, представляются важными для формирования рациональной программы действий специалистов на разных этапах построения системы защиты — от формирования политики безопасности до эксплуатации и поэтапной модернизации системы.

Сформулируем в самом общем и кратком виде положения, которые могут рассматриваться как отправные (начальные) для формирования модели атаки, проявления которой могут быть охарактеризованы как кибертерроризм.

Рассматривая набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих «типовой профиль» такого сценария можно выделить следующие:

- субъект действия — персона и (или) группа лиц, имеющих целью проведение террористических действий против объекта (объектов), и (или) совокупность их агентов на сетевой среде первичного объекта атаки (определение далее по тексту), действующих с использование скрытых каналов передачи информации [22];
- предмет действия — сетевая инфраструктура (физическая среда передачи данных, коммуникационные средства и программное обеспечение), предоставляющие доступ к информационно-вычислительным ресурсам системы;
- цель действий — использовать предмет действия (сетевую инфраструктуру) для деструктивного воздействия на объект (объекты), результатом которого будут различные последствия (почва для шантажа, покушение на жизнь людей, разрушение вторичных объектов и т. п.);
- первичный объект —
  - компьютерный комплекс для относительно узкой, но стратегически важной или, например, способной прямо влиять на здоровье людей, области применения;
  - большая интегрированная система распределенных информационно-вычислительных ресурсов для обслуживания национально значимой сферы деятельности (сектора экономики, промышленности, ...), например энергетическая (в т. ч., атомная), транспортная (воздушная или железнодорожная) система или её элементы (местные, региональные);
- вторичный объект — персона или группа людей, материальные объекты различного назначения, информационные системы, которые могут быть подвержены деструктивным воздействиям со стороны первичных объектов, вплоть до уничтожения.

Усредненный сценарий действий террористов при этом должен, как правило, содержать:

- действия, обеспечивающие неавторизованный доступ к информации с высоким уровнем секретности;
- уничтожение, модификацию или замену программного кода, обеспечивающего нормальное (регламентированное) функционирование системы;
- ограничение доступа внешних или внутренних агентов системы безопасности, способных оперативно предотвратить злоумышленные действия.

Конечно, представленные положения не позволяют сформулировать модель атаки с надлежащей степенью полноты. Это предмет более глубокого анализа специалистов разных (в том числе гуманитарного цикла) направлений. Однако, и они позволяют описать основные типы угроз, предсказать условия их реализации, а значит, и общие соображения, которые могут быть положены в основу модели противодействия атаке. Следует отметить, что налицо комбинация всех трех типов угроз, соответственно, — конфиденциальности, целостности и доступности, на предотвращение которых должны быть ориентированы системы информационной безопасности рассматриваемых комплексов. Важным фактором эффективности противодействия выступает необходимость оперативной, в реальном времени реакции на последовательность вышеперечисленных действий с атакующей стороны.

К разработке модели противодействия

Рассмотрим общие положения модели защиты, как системы контрмер, которые необходимо предпринимать на всех уровнях реализации сетевой безопасности для предотвращения каждой из перечисленных выше угроз и их совокупности в контексте «среднего» сценария террористического акта. Главной задачей на административном уровне является выработка подходов к формированию политик безопасности для распределенных, вообще говоря, гетерогенных систем, интегрирующих в своем составе подсистемы с различными функциями и условиями эксплуатации.

В числе первых действий на операционном, а тем более, программно-техническом уровне обеспечения информационной безопасности, должна стать выработка (на основе анализа основных положений современных критериев оценки безопасности информационных технологий) заданий на безопасность и профилей защиты, которые отвечали бы политике безопасности систем, подлежащих защите от кибертеррористических атак.

Как результат более эффективных мер, которые будут способны противостоять (противодействовать) угрозе конфиденциальности (неавторизованному доступу к информации высокого уровня секретности или элементам управляющей инфраструктуры) могут рассматриваться:

- на операционном уровне — это обучение и управление персоналом, четкое распределение обязанностей и минимизация привилегий;
- на программно-техническом уровне — средства идентификации и аутентификации пользователей, учитывающие их индивидуальные особенности; управление ресурсами на основе комбинации традиционных и новейших моделей логического разграничения доступа, учитывающих различные требования по безопасности к разным компонентам системы, а также криптографическая поддержка и экранирование.

Угрозе целостности информации должны противодействовать специальные программно-технические меры, контролирующие целостность и согласованность данных при их хранении и передаче. Отражению атак (угроз) на доступность способствуют такие меры, как оперативная реакция на сбои и механизмы надежного восстановления — на операционном уровне, повышенные меры отказоустойчивости, распределение и квотирование ресурсов — на уровне программно-технических сервисов.

Для предотвращения всех трех типов угроз на операционном уровне очень важной является физическая защита (включая физическое управление доступом) ключевых элементов сетевой инфраструктуры, а на программно-техническом уровне — протоколирование и активный аудит системы на предмет обнаружения аномальных ситуаций, способных деструктивно повлиять на ее функциональность. Своевременное обнаружение, оперативное и адекватное реагирование на подобные ситуации обеспечивает более высокий уровень безопасности (защищенности).

Отдельного внимания в плане формирования общей модели противодействия кибертерроризму заслуживают примыкающие к программно-техническим сервисам вопросы, связанные с выработкой системы в организации аудита недоверенных технических средств и программного обеспечения.

Настоятельная потребность в аудите и сертификации аппаратных средств, которые используются в национально значимых компьютерных системах, объясняется отсутствием доверенных зарубежных или отечественных аналогов.

Внимание, особенно в последние годы, к верификации программ обусловлено не столько стремлением исправлять «ошибки» (хотя и этим обстоятельством), сколько широким использованием программных систем со свободно распространяемыми в Интернет кодами. Такое программное обеспечение (и системное, и прикладное), как правило, разрабатываемое с участием широкого круга специалистов из разных стран мира, либо напрямую используется в комплексах различного назначения, либо на его основе идет разработка доверенного программного обеспечения.

Замечу, что приведены не все основные меры, способные противодействовать перечисленным угрозам. Их сложно систематизировать и обобщить в одной статье. Отметим мероприятия, обобщающие их в рамках отдельных уровней.

К мерам общего характера на этом направлении можно отнести следующие:

- Разработка новых законодательных актов (национальных и международных) в области контроля над использованием систем сетевого управления национально значимыми сферами хозяйственного комплекса, оборонной промышленности и бизнеса с точки зрения возможного применения в отношении них террористических действий.
- Поиск типовых подходов к формированию
  - политик безопасности для стратегически важных объектов, управление которыми осуществляется с использованием сетевых структур, на основе анализа рисков, связанных с террористическими действиями (актами);
  - программ практической реализации политик безопасности и операционных регуляторов, ориентирующих персонал, обслуживающий системы управления

такими объектами, на неукоснительное соблюдение правил, выработанных для их выполнения.

- Строгое следование требованиям и критериям стандартов (национальных и (или) международных) оценки продуктов или систем, предназначенных для эксплуатации на сетевой среде в условиях, предусматривающих оперативную реакцию на террористические действия.
- Анализ существующих показателей безопасности сетевых продуктов и систем с позиции их адекватной реакции на возможные сценарии террористических действий, развитие уже существующих стандартов в этой области на основе проведенного анализа.

Мировая сеть Интернет, построенная на основе стека протоколов TCP/IP, транснациональна по своей природе. Изначально рассчитанный на использование в открытых исследовательских и образовательных сетях, базовый в Интернет протокол межсетевого взаимодействия IPv.4, до настоящего времени имеет проблемы с защитой информационных ресурсов и защитой инфраструктур, поддерживающих такие сети. Несмотря на большую, многолетнюю (более 20 лет) работу, проводимую мировым сообществом математиков и программистов, исследователей и практиков, значительная их часть не устранена до настоящего времени.

Однако темпы роста метасети Интернет огромны. Сегодня она объединяет более 200 млн. сетевых ЭВМ в почти 250 странах мира на всех континентах. Эта сеть «де-факто» или потенциально имеет связность с любыми сетями от локальных бытовых и исследовательских до сетей силовых ведомств или сетей, которые используются для управления национально значимыми отраслями или сферами деятельности. Это безусловно инфраструктура, которая потенциально может быть задействована террористами для реализации своих целей в каждой из перечисленных выше сфер и отраслей человеческой деятельности. Более того, чем выше уровень развития сетевых технологий, шире спектр их использования в различных сферах человеческой деятельности, тем вероятнее внимание к ним со стороны террористов и более изощренны могут быть их действия. Сегодня, например, не выглядит нереализуемым намеренно организованный отказ бортовой системы управления транспортным средством в воздухе, на земле или на воде, выдача управляющих воздействий, которые могли бы перенацелить боевые снаряды (ракеты) на другие цели.

К сожалению, такие примеры можно продолжить. С этим нужно считаться и предвосхищать подобные действия.

Проблемы реализации

Представленные в настоящей работе идеи и положения следует рассматривать как результат начального осмысления очень важной и трудной для решения проблемы. Исходная посылка о том, что в методическом плане традиционные подходы к разработке и построению систем информационной безопасности остаются неизменными при создании систем и сценариев противодействия кибертерроризму, не только не отменяются, а наоборот, требует более серьезного осмысления этой базы. В данном контексте совершенствование критериальной основы оценки безопасности информационных технологий, разработка новых конструктивных моделей для тестирования, верификации средств защиты сложно организованных распределенных компьютерных систем, формирование доказательной базы их гарантированной защищенности, совершенствование программно-технических сервисов безопасности — это движение в правильном направлении. Однако трудности на этом пути есть. Приведу лишь две из них, которые указывают на стратегический и даже глобальный характер проблемы.

- Многие из обсуждаемых выше положений, призванных сформировать адекватные подходы к описанию политики безопасности, моделей (профилей) атаки и атакующего, модели защиты в условиях противодействия кибертерроризму, пока не обеспечены соответствующими технологическими средствами. Трудность состоит не только в разработке упомянутых конструктивных моделей (что представляет большую комплексную задачу), но и в поиске теоретических подходов к созданию технологий и инструментальных средств для реализации отдельных механизмов этих моделей. Работа на этих направлениях потребует привлечения современных математических методов и совместной, скоординированной работы математиков, специалистов в области информационной безопасности и сетевых технологий.
- Ряд крупных, рассматриваемых в качестве потенциально уязвимых для кибертерроризма, национально значимых систем взаимосвязаны на основе современных магистральных сетевых

инфраструктур транснационального масштаба. Это обстоятельство делает потенциально более подверженными в отношении указанных угроз страны с низким уровнем развития сетевой инфраструктуры. Во-первых, эти страны уязвимы к подобным действиям на их собственной территории. Во-вторых, как в случае с традиционным «хакерским» приемом, когда в качестве «транзитного» для атаки используется какой-то третий компьютер со слабой системой защиты. В качестве таковых для крупных террористических действий (включая их подготовку) могут использоваться элементы сетевой инфраструктуры слаборазвитых в сетевом отношении стран. Такое развитие событий возможно, оно требует осмысления и выработки программы действий на международном уровне. Это не простое механическое переосмысление, например, политики, проводимой ЮНЕСКО в рамках соответствующей программы по выравниванию сетевых инфраструктур различных стран за счет помощи странам, слабым в этом отношении. Проблема информационной безопасности (сетевой в том числе) более тонкая и серьезная. Она, кроме общих (в методологическом, техническом, правовом и т. п. плане) межнациональных, затрагивает и национальные интересы. Поэтому их реализация потребует выработки некоторых сбалансированных в этом отношении мер и программы. Однако тот факт, что такая программа необходима, сомнений не вызывает и это прекрасное поле для активных совместных действий на международной арене.

Заключение

В заключении хотелось бы заметить, что описанные выше сценарии действий могут быть обусловлены не только террористическими целями. Однако проблема в целом и условия ее разрешения при этом не изменяются.

Представленные в настоящей работе материалы не претендуют на полноту изложения и отточенность формулировок. Это в большей степени «эскизный проект» или предложения для активных действий на новом, актуальном и продиктованном самой жизнью направлении.

Основные идеи, положения и оценки прошли осмысление и некоторую апробацию при обсуждении вопросов на семинарах и «круглых столах» по проблемам информационной безопасности

в Московском университете, на конференциях «Московский университет и развитие криптографии в России» и «Математика и безопасность информационных технологий» (МаБИТ-03). Все эти обсуждения стали возможны благодаря тому, что тематика информационной безопасности была принята, получила одобрение и развитие в научном и образовательном плане в МГУ им. М. В. Ломоносова. Инициатором этого процесса с 1997 года стал ректор Московского университета академик Виктор Антонович Садовничий. Благодаря его поддержке, участию в исследованиях и активной позиции в плане развития учебного процесса, к данной тематике привлечены математики и специалисты в области кибернетики, физики и экономисты, психологи, юристы и политологи. Такое положение дел является гарантией новых, интересных, в том числе — междисциплинарных результатов, на которые в значительной степени рассчитана программа действий, кратко изложенная в данной работе.

Литература

[1] Высокотехнологичный терроризм. Материалы российско-американского семинара. Москва, 4–6 июня 2001 г., Российская академия наук в сотрудничестве с Национальными академиями США, 320 с.

[2] *Васенин В. А.*, *Галатенко А. В.* Компьютерный терроризм и проблемы информационной безопасности в Интернет // Высокотехнологичный терроризм. Материалы российско-американского семинара РАН в сотрудничестве с Национальными академиями США. Москва, 4–6 июня 2001 г., М., 2002, с. 211–225.

[3] *Васенин В. А.*, *Галатенко А. В.* О проблемах информационной безопасности в сети Интернет. Глобальная информатизация и безопасность России. Материалы круглого стола «Глобальная информатизация и социально-гуманитарные проблемы человека, культуры и общества. МГУ, октябрь 2000 г., М.: Изд-во МГУ, 2001, с. 199–214.

[4] Trusted Computer System Evaluation Criteria, US DOD 5200. 28-STD, December 1985.

[5] National Computer Security Center. A Guide to Understanding Audit in Trusted Systems // NCSC-TG-001, 1987.

[6] National Computer Security Center. A Guide to Understanding Audit in Trusted Systems // NCSC-TG-003, 1987.
[7] National Computer Security Center. Trusted Network Interpretation // NCSC-TG-003, 1987.
[8] Security Architecture for Open Systems Interconnection for CCITT Applications / Recommendation X.800 // CCITT. Geneva, 1991.
[9] Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France—Germany—the Netherlands—the United Kingdom // Department of trade and Industry. L., 1991.
[10] Canadian Trusted Computer Product Evaluation Criteria. Version 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada. January, 1993.
[11] Information Technology Security Evaluation Criteria. Version 1.2. Office for Official Publications of the European Communities. June 1991.
[12] Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от несанкционированного доступа к информации. М., 1992.
[13] Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.
[14] Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.
[15] Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. М., 1992.
[16] Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.
[17] Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. — ISO/IEC 15408 — 1.1999.
[18] Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements. — ISO/IEC 15408 — 2.1999.
[19] Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements. — ISO/IEC 15408 — 3.1999.
[20] Проект Госстандарта РФ ГОСТ Р ИСО/МЭК 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.» Части 1, 2, 3. М.: Изд-во Госстандарта России, 2002.
[21] *Грушо А. А.*, *Тимонина Е. Е.* Теоретические основы защиты информации. М.: Изд-во агентства «Яхтсмен», 1996. 192 с.
[22] *Грушо А. А.*, *Тимонина Е. Е.* Языки в скрытых каналах. Труды международной конференции «Информационные технологии в науке, образовании, телекоммуникациях, бизнесе». Украина, Крым, Ялта—Гурзуф, 19–29 мая 2003 г.

Война или мир: международные аспекты информационной безопасности

А. В. Крутских

Значение информации как таковой, а также оперативного доступа к ней в рамках политической борьбы или экономической конкуренции, во все времена было априори победоносным фактором. Будь то во внутренней жизни государств или на международной арене. Применительно к XXI веку, который характеризуется переходом человечества в своем развитии от стадии «индустриального» общества к обществу «информационному», можно с уверенностью сказать, перефразируя известного классика: **Информация решает все!**

В чем же угроза?

В условиях объективно формирующегося глобального информационного пространства, существо проблемы международной информационной безопасности (МИБ) коренится в лавинообразном процессе развития и внедрения новейших информационных, телекоммуникационных и кибернетических технологий. Обеспечивая беспрецедентные возможности накопления и использования информации, эти технологии и средства одновременно создают фундаментальную зависимость от их нормального функционирования всех сфер жизнедеятельности общества и государства: экономики, политики, культуры, обеспечения национальной и международной безопасности.

Мировая информационно-технологическая революция наряду с очевидными благами, которые она уже дала человечеству, одновременно создает принципиально новые потенциальные угрозы использования достижений научно-технической мысли в этой области в целях, несовместимых с задачами поддержания

международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека.

Озабоченность возникает, прежде всего, в связи с возможностью применения колоссального потенциала информационно-кибернетических технологий в интересах обеспечения военно-политического превосходства, силового противоборства, шантажа. Увеличение за счет новейших информационных технологий военного потенциала развитых стран ведет к изменению глобального и региональных балансов сил, напряженности между традиционными и нарождающимися центрами силы, появлению новых сфер конфронтации. Возникает соблазн воспользоваться преимуществами в обладании информационными технологиями для информационной, политической, экономической, культурной и военной экспансии. С другой стороны, страны вовлекаются в процесс создания у себя потенциала для «международного хакерства», «информационного пиратства» и агрессии. К этой деятельности уже подключились радикалистские политические группировки, «новый» оружейный бизнес, а наряду с ними — террористические и криминальные организации и группы.

Не исключено, что уже в обозримом будущем карательные акции на международной арене будут осуществляться против отверженных не при помощи крылатых ракет и воздушных бомбардировок, а с использованием информационного оружия. И тогда любые действия, подпадающие сегодня под статус конфликтов, примут характер информационных войн.

Изощренные сценарии применения информационного оружия, пока к ним не стали привыкать, захватывали дух при просмотре фильмов «ужастиков», рисовавших картины того, как оживали компьютерные вирусы, заранее тайно заложенные в электронные системы государственного, экономического и военного управления, практически полностью парализуя их; как с помощью электронных средств злоумышленники, действуя с расстояния в тысячи километров, обнуляли банковские счета целых государств и выводили из строя важнейшие объекты промышленности, связи, энергетики, транспорта, коммунального хозяйства, экологического контроля (например, атомные электростанции, аэропорты, пункты управления стратегическими силами); как, используя мощные генераторы электромагнитных импульсов, удавалось разрушать программное обеспечение и уничтожать важные

базы данных защищенных компьютерных систем; как сеялась паника среди населения и дезинформировалось руководство страны.

И вот теперь, постепенно, телесказки начинают получать реальное воплощение. Еще в середине 80-х годов был предан огласке факт о том, что во время американо-иранского кризиса, вызванного захватом американских заложников в Тегеране, США удалось с помощью специальной компьютерной программы практически мгновенно заблокировать все зарубежные счета этой страны. Эффективность и масштабы применения средств радиоэлектронной борьбы против Багдада во время карательной операции «Буря в пустыне» дали основание военным специалистам считать Ирак примером первой «информационной Хиросимы». Последним полигоном информационно-электронной войны стала Югославия.

Целенаправленное информационное воздействие на противника (конкурента, оппонента) старо как мир. Однако только сейчас, благодаря новейшим технологиям, оно эволюционирует от отдельных информационных диверсий и акций по дезинформации во вполне оформившийся способ обеспечения международной политики, отличающейся массированным, тотальным характером применения.

Настораживающее впечатление производят в этом контексте данные главного контрольно-финансового управления Конгресса США, согласно которым сейчас примерно 120 стран мира ведут работы или уже завершили отдельные разработки по развитию возможностей информационно-компьютерного воздействия на информационный ресурс потенциального противника. Для сравнения: разработки в области ядерного оружия ведутся не более чем в 20 странах.

* * *

Таким образом, прогресс в информационных технологиях, так же как ранее в ядерных, чреват новым витком гонки вооружений, который вновь может отвлечь огромные ресурсы человечества от целей мирного созидания.

Усугубляется проблема обеспечения международной информационной безопасности тем, что она еще не стала объектом всестороннего регулирования в рамках международного права.

Особенности «чудо-оружия»

Пока в мире не выработано общепринятого определения «информационного оружия». Известно, что этот термин впервые стал употребляться в американских военных кругах в 1991 году, после окончания войны в Персидском заливе. Осложняет вопрос дефиниций то обстоятельство, что информационные технологии большей своей частью выступают как технологии двойного или даже вообще невоенного назначения. По мнению многих экспертов, массированные информационные агрессии могут осуществляться с помощью обычных персональных компьютеров с использованием широких технологических возможностей Интернет.

Особенность процесса информационной милитаризации заключается в том, что она происходит через конвергенцию гражданских и военных технологий и «реверсирование» их внедрения, т. е. они первоначально появляются и, главным образом, задействованы в гражданском секторе, и лишь потом или вообще на время переходят в военный.

К характерным чертам информационного оружия можно отнести его качественную универсальность, радикальность воздействия, доступность. Оно отличается широким выбором времени и места применения. Для его приведения в действие не требуется больших армий, что делает информационную войну сравнительно экономичной. Его применение носит обезличенный характер, легко маскируется под обычную деятельность. Одновременно трудно определить его «обратный адрес» и национальную принадлежность. Агрессия может фактически осуществляться государствами «чужими руками» или таким образом, что в качестве ответственного за информационное нападение будет подставляться невиновное государство.

Информационное оружие не знает географических расстояний, подрывает традиционное понятие государственных границ, делая их технологически проницаемыми. Использование этого оружия может происходить весьма скрытно («буднично»), не доводя дело до объявления «горячей» войны; не нуждается в большой и видимой подготовке. Подчас жертва может даже не осознавать, что находится под информационным воздействием. К тому же, в связи с отсутствием систем и методик, оценивающих угрозу и заранее предупреждающих о готовящемся нападении, осложняется возможность противодействовать такой агрессии.

Наиболее опасно применение информационного оружия против военных и гражданских объектов и структур, которые должны находиться в состоянии непрерывной работоспособности и функционировать в реальном масштабе времени (системы раннего предупреждения о воздушно-космическом нападении; системы управления ПВО, ПРО, СЯС; энергетические комплексы, особенно ядерные; промышленные производства). Результаты враждебного воздействия на их работу могут иметь катастрофический характер и по возможному ущербу быть сопоставимы с последствиями применения оружия массового уничтожения! Например, взламывая электронную защиту, вызывать «эффект Чернобыля».

Информационное оружие революционизирует международный конфликт как таковой. В ходе локальных столкновений, с его помощью становится возможным обходиться без занятия территорий, не иметь дело с проблемой военнопленных, уменьшать собственные потери, передоверяя инициативу в решении боевых задач информационно-электронным и безэкипажным средствам.

Хотелось бы отметить псевдогуманную сторону информационной войны. Многие методы ее ведения, например вывод из строя телекоммуникационных систем, запуск вирусных программ, создание технических помех, блокирование связи и т. д., нанося ощутимый экономический ущерб, непосредственно не приводят к кровопролитию, жертвам, видимым разрушениям, сопутствующим обычным военным действиям. В результате их применения никто напрямую не лишается крова, пищи и прочих вещей, элементарно необходимых для поддержания жизни. В такой ситуации, по всей вероятности, не возникнет и проблема беженцев. А значит — все это может вести к снижению моральных порогов при принятии политического решения о нанесении «информационного» удара.

Одновременно, распространение ореола «гуманности», технократичности вокруг информационно-кибернетических средств и методов военно-политического воздействия — способно породить в мире опасную беспечность и терпимость в отношении их применения, большую снисходительность к использованию в международных отношениях одним государством против других односторонних санкций, если последние формально будут основываться на электронике, а не на крови.

Импонировать обывателю может и то, что развитие военно-информационных возможностей не связано с наращиванием огромных вооруженных сил и даже, наоборот, ведет к их сокращению, выступает в качестве объективной дани техническому прогрессу. Плюс ассигнования на эти цели легко маскируются и реализуются в рамках колоссальных мирных программ.

Отдельно требуется сказать о возможных угрозах правам и свободам граждан, реализуемым в области духовной жизни и информационной сфере. Формально, «без какой-либо политики», сугубо технологически можно свести на нет одно из величайших завоеваний демократии — право на свободу информации и деятельности СМИ. Здесь же следует упомянуть угрозу системам сбора и хранения данных о личности: медицинская информация, метрические данные, сведения о занятиях и доходах граждан и т. п. Кроме того, в правовом обществе должна обеспечиваться конфиденциальность информации о частной жизни и приватного информационного обмена между частными лицами.

Использование информационных технологий одним государством против другого вполне может быть квалифицировано как акт информационной войны, если не войны вообще.

Информационный джинн нуждается в контроле

Осознание того факта, что появление и распространение информационного оружия, милитаризация информационных технологий явятся мощным дестабилизирующим фактором международных отношений и подвергнут серьезному испытанию всю систему международных договоренностей по поддержанию стратегической стабильности, в т. ч. и на региональных уровнях; стремление выйти из губительного цикла гонки новых технологических вооружений и перевести процессы гражданской и военной информатизации в плоскость международно-правового регулирования *побудили Россию взять на себя инициативу в рамках мирового сообщества в официальной постановке вопроса об обеспечении международной информационной безопасности*, причем сделать это, как говорится, по всем азимутам.

Первым и небезуспешным шагом российской дипломатии на этом поприще стала попытка убедить США — одного из ключевых игроков на мировом информационном поле — в том,

что информационно-технологические процессы могут иметь существенную негативную оборотную сторону и, следовательно, не должны развиваться самотеком без адекватного международного контроля.

В принятом в сентябре 1998 года на встрече президентов России и США совместном Заявлении с весьма символическим названием «Об общих вызовах безопасности на рубеже XXI века», констатировалось согласие активизировать совместные усилия по противодействию транснациональным угрозам экономике и безопасности наших стран, включая преступления с использованием компьютерной техники и других высоких технологий; признавалась также важность содействия положительным сторонам и ослабления действия отрицательных сторон происходящей сейчас информационно-технологической революции, что является серьезной задачей в деле обеспечения стратегических интересов обоих государств в будущем.

Хотя в дальнейшем, на уровне дипломатических экспертов Соединенные Штаты заняли явно выжидательную позицию, выделяя в качестве приоритетных для себя лишь криминальные и террористические аспекты проблемы и затушевывая ее военную составляющую, — нельзя исключать, что под воздействием объективных обстоятельств в области мировой информатизации, тема информационной безопасности станет одной из важнейших в наших переговорах с США по вопросам стратегической стабильности и будущего наших взаимоотношений.

Конструктивный обмен мнениями на основе совпадения принципиальных подходов и оценок по МИБ поддерживается Россией с подавляющим большинством государств мира, а также Китаем и странами СНГ, с которыми мы разделяем практически единое информационное пространство.

Учитывая масштабы глобального информационного вызова, ставящихся им проблем невозможность их решения усилиями одной или нескольких стран, как на блоковой основе, так и по принципу «спасайся кто может» (в силу неделимости мирового инфопространства; если, конечно, не обрекать себя на самоизоляцию в мире), — российская сторона активные действия сосредоточила в ООН. Это глобальная организация, способная обеспечить решение любой политической проблемы комплексно, при самом широком представительстве и максимальном учете интересов стран-членов.

Заметной вехой в этой работе послужил вклад Министра иностранных дел России И. С. Иванова, направившего 23 сентября 1998 года специальное Послание по проблеме международной информационной безопасности Генеральному секретарю ООН и выдвинувшего на этот счет в ходе 53-й Сессии Генеральной ассамблеи ООН соответствующий проект резолюции. Принятый 4 декабря 1998 года консенсусом, этот документ (№ 53/70) под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», по существу, стал началом обсуждения создания совершенно нового международно-правового режима, субъектом которого в перспективе должны стать информация, информационная технология и методы ее использования.

Обновленный вариант этой резолюции (№ 54/49), принятый Генеральной ассамблеей ООН 1 декабря 1999 года также консенсусом, не только констатировал наличие общей для человечества проблемы МИБ, но и прямо указывал на ее военное и, соответственно, политическое измерение.

Стремясь заложить конструктивные направляющие для предметного международного обсуждения тематики МИБ, российская дипломатия подготовила и внесла в ООН два концептуальных документа — доклад Генеральному секретарю ООН о российской позиции по данной проблеме (9 июня 1999 года) и «Принципы, касающиеся международной информационной безопасности» (май 2000 года). В них даются определения основных угроз в сфере МИБ; формулируются направления по продвижению, задачи, цели и принципы разработки соответствующего международно-правового режима; предлагается базовый понятийный аппарат.

Этой деятельности противостоит вполне реальная оппозиция, организуемая главным образом рядом ведущих стран НАТО. Уже не отрицая в целом наличия проблемы, они ссылаются на то, что вопрос для конкретного рассмотрения, мол, «не созрел», прикрываются отсутствием отработанной методики контроля, высказывают опасения о возможном нанесении ущерба свободе обмена информацией и конкуренции на рынке инфотехнологий. Возможность создания информационного оружия и угроза возникновения информационных войн ими принижается. Отрицается, соответственно, и разоруженческий аспект проблемы. Проталкивается идея сегментирования темы и перевода ее

обсуждения из Первого (политический плюс вопросы разоружения и безопасности) во Второй (экономический) и Шестой (правовой) комитеты Генеральной ассамблеи ООН, а также рассредоточения по региональным и тематическим форумам («восьмерка», Евросоюз, Интерпол, ОАГ и т. д.). При этом, когда российская сторона действительно предложила внести тему МИБ на рассмотрение саммита «восьмерки» 2000 года, наши партнеры в рамках данного форума продемонстрировали готовность обсуждать по существу только экономическую сторону мирового информационного процесса.

Иначе говоря, мировые «силовики» по-прежнему намерены сдерживать углубление содержательной части дискуссии вокруг МИБ, сохраняя тем самым свободу для своих дальнейших разработок в сфере военного применения информтехнологий.

В такой дипломатии большинство стран мира, особенно развивающиеся, усматривают угрозу их изоляции от активного участия в решении проблемы, а кроме того — попытку консервации их уязвимости от информационной агрессии. Они солидаризируются с российской концепцией изучения проблемы в комплексе, с выделением приоритетности потенциальной угрозы информационной войны.

Обозначается определенный диссонанс и в позициях многих развитых государств. Реальности современной жизни все больше убеждают их, что даже статус союзника США не гарантирует их от электронного проникновения со стороны своего «большого брата», причем последнее может оказываться далеко не бескорыстным.

В целом ряде стран Западной Европы ведутся официальные расследования по поводу деятельности против них принадлежащей американскому правительству системы электронной разведки, прослушивания, промышленного шпионажа, сбора стратегической, в т. ч. коммерческой и частной, информации — «Эшелон».

В процессе двусторонних консультаций по МИБ, приходится подчас слышать и такие суждения, когда отдельные умы, «подхватывая» нашу инициативу, выступают с крайне радикальных, порой взаимоисключающих позиций — от полного запрещения уже сейчас всех информационных технологий, способных применяться в военных целях, до призывов обратить это «изобретение Запада» против него самого. Очевидно, что такие подходы могут

привести к конфронтации в ООН, блокированию поиска решения этой проблемы вообще.

Результирующая политической борьбы по проблеме МИБ на сегодняшний день заключается в том, что международное сообщество вполне понимает ее существо и актуальность, признает необходимость воспользоваться моментом, созданным российской инициативой, для создания совместными усилиями международных организационно-правовых условий или, своего рода, кодекса поведения государств в информационном пространстве для цивилизованного развития технологического прогресса в мире.

Убедительным свидетельством заряженности ООН на широкое международное взаимодействие по МИБ стало принятие ее Генеральной ассамблеей, опять же консенсусом, 20 ноября 2000 года соответствующей, предложенной Россией, резолюции. В ней удалось отстоять важнейшее положение о необходимости изучения международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем, *а также обратиться с призывом ко всем государствам-членам содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности и мер по их ограничению*.

Данная резолюция придала мощный импульс рассмотрению проблематики МИБ на национальном уровне: большинство ключевых в информационном плане государств представили в Секретариат ООН документы, содержащие оценки по вышеперечисленным вопросам, и вошедшие в соответствующие доклады Генсекретаря ООН. Среди них — США, Европейский союз, Австралия, Великобритания, Куба, Мексика, Гватемала, Филиппины, Белоруссия, Украина. Россия направила четыре развернутых документа по различным аспектам МИБ.

Итогом этой международной деятельности, инициированной российской стороной, явилось *принятие 8 декабря 2003 года Генассамблеей ООН традиционно консенсусом резолюции, переводящей общеполитическое обсуждение вопросов МИБ в плоскость поиска практических решений. Эта резолюция запускает механизм формирования Группы правительственных экспертов ООН по МИБ*. Ее первое заседание намечено на июль 2004 года.

Мандат Группы предусматривает проведение исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также изучение международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем. Результатом работы Группы станет доклад Генсекретаря ООН Генеральной Ассамблее в 2005 году о результатах данного исследования, который задаст рамки и определит направления международного сотрудничества в целях формирования режима МИБ.

Построение МИБ

(из документа № A/54/213, внесенного Россией в ООН 9 июня 1999 года)

a) определение признаков и классификация информационных войн;
b) определение признаков и классификация информационного оружия, а также методов и средств, которые можно отнести к информационному оружию;
c) ограничение оборота информационного оружия;
d) запрещение разработки, распространения и применения особо опасных видов информационного оружия;
e) предотвращение угрозы возникновения информационных войн;
f) запрещение использования информационных технологий и средств во враждебных целях и, в частности, против согласованных категорий объектов;
g) признание сравнимости применения информационного оружия в отношении критически важных структур с последствиями применения оружия массового поражения;
h) создание условий равноправного и безопасного международного информационного обмена на основе баланса интересов личности, общества и государства;
i) предотвращение угроз использования информационных технологий и средств в террористических и других преступных целях;
j) предотвращение угрозы использования информационных технологий и средств для воздействия на общественное сознание с целью дестабилизации общества и государства;

k) разработка процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;
l) создание механизма разрешения конфликтных ситуаций в сфере информационной безопасности;
m) создание международной системы сертификации технологий и средств информатизации (в том числе программно-технических) в части гарантий их информационной безопасности;
n) развитие системы международного взаимодействия правоохранительных органов по предотвращению преступлений в информационной сфере;
o) создание механизма контроля за выполнением условий режима международной информационной безопасности;
p) гармонизация национальных законодательств в части обеспечения информационной безопасности.

Методологические проблемы противодействия кибертерроризму

А. А. Сальников, В. В. Ященко

В последние годы в мире наряду с позитивными процессами, связанными с глобальной информатизацией и созданием условий для построения информационного общества, идут негативные процессы, связанные с милитаризацией и криминализацией информационного пространства. Глобальные информационно-телекоммуникационные системы и информационно-кибернетические технологии становятся высокоэффективным средством и орудием для достижения военно-политических, криминальных и террористических целей. Поэтому для своего устойчивого развития человечество должно найти механизмы противодействия этим новым угрозам, разработать, обосновать и реализовать комплекс мер по обеспечению безопасности в информационном пространстве.

Поскольку новые угрозы носят транснациональный и трансграничный характер, важнейшим средством противодействия этим угрозам являются международно-правовые механизмы обеспечения информационной безопасности — проблемам их разработки посвящена обстоятельная статья А. В. Крутских в настоящем сборнике.

Следует подчеркнуть, что при анализе проблем противодействия кибертерроризму необходимо более чётко отделять кибертерроризм от других угроз безопасности. В частности, использование глобальных информационно-телекоммуникационных систем только в качестве инфраструктуры для планирования и управления проведением террористических актов не может быть отнесено к кибертерроризму. Важнейшим признаком кибертерроризма является использование информационно-телекоммуникационнных систем в качестве орудия для террористического акта. Поэтому одним из необходимых элементов кибертерроризма является кибернетическая (компьютерная) атака. Но с другой стороны, кибератаки могут проводиться не только

в террористических целях — они могут проводиться хакерами в хулиганских или криминальных целях, а также спецслужбами в военно-политических целях. При этом с технической точки зрения кибератаки, проводимые в различных целях, могут и не отличаться — в канале, в сети и в компьютере может проявиться только уровень мастерства атакующего и эффективность применяемых им средств. Более подробно на технических, программистских аспектах противодействия кибертерроризму мы останавливаться не будем — отсылаем читателя к обстоятельной статье В. А. Васенина в настоящем сборнике.

При рассмотрении информационных технологий с позиций безопасности существенную роль играет их дуализм: с одной стороны, информационно-телекоммуникационные системы и технологии могут рассматриваться как объект нападения, с другой стороны — как оружие в руках террористов, противников или преступников, а иногда эти системы и технологии выступают как то и другое одновременно. Именно поэтому сложно провести чёткую грань между кибертерроризмом, использованием информационных технологий в военно-политическом противостоянии и другими видами киберпреступлений. Кибертерроризм отличается от других форм преступных воздействий на информационную среду прежде всего своими целями, которые свойственны терроризму вообще. Террористы стремятся к тому, чтобы их теракты

1) имели опасные последствия;
2) стали широко известны населению;
3) имели большой общественный резонанс;
4) создали атмосферу угрозы непредсказуемого повторения теракта.

Угроза инфогенных катастроф мирового масштаба в случае удачно проведенных кибератак террористов требует согласованных действий всего мирового сообщества по противодействию этим угрозам. По существу, сегодня уже начата работа по созданию нового международно-правового режима, субъектом которого должны стать информация, информационные технологии и методы их использования. Не последнюю роль в этой работе имеет проблема создания базового понятийного аппарата — необходимо договориться о единой трактовке терминов, используемых в этой специфичной области. Необходимо стремиться к гармонизации национальных законодательств в части борьбы с кибертерроризмом и киберпреступлениями вообще.

Совсем непросто будет выработать единую систему мер противодействия международному терроризму в международном масштабе. Так, в частности, даже внутри отдельной страны — США — законодательно ограничен обмен информацией между частными корпорациями о компьютерных атаках, что не позволяет учиться на опыте друг друга.

Неординарность новых угроз безопасности киберпространства может потребовать от международного сообщества и неординарных мер противодействия. Одной из таких мер может стать использование потенциала хакерского сообщества в антитеррористических целях. При этом мы трактуем хакерство не только как сообщество киберхулиганов и киберпреступников, а шире — как сообщество людей с ярко выраженным (иногда и гипертрофированным) увлечением к познанию в области информационных технологий, выходящим за рамки познавательной и учебной деятельности. Для привлечения таких неформальных сообществ к борьбе с международным кибертерроризмом необходимо обратить самое серьёзное внимание на выработку позитивной мотивации одарённой молодёжи. В мотивах действий хакеров психологи выделяют:

— любопытство;
— удовольствие, получаемое от ощущения силы;
— узнавание в киберпространстве таких же, как ты;
— переживание опыта потока, т. е. особого психологического состояния включённости в деятельность, при котором действия и их осознание сливаются для субъекта в одно целое, а результат деятельности отходит на задний план.

Все эти мотивы могут иметь для общества как положительную, так и отрицательную направленность. Необходимо привлечь психологов, педагогов, социологов, специалистов mass-media для разработки систем мер, направленных на положительную ориентацию «кибернеформалов». Задача формирования представлений о добре и зле, «моральных заповедей» поведения в киберпространстве психологически не проста. Опосредованность, разделение во времени и пространстве приводит к сильному изменению представлений об антигуманности тех или иных действий в киберпространстве: сидя за монитором компьютера, человек отстранён от последствий и непосредственно не наблюдает того ущерба, который он наносит своими преступными действиями другим людям.

Считаем важным разработать систему мер по мониторингу и контролю за распространением знаний и технологий, критичных с точки зрения информационной безопасности. Один из основных ресурсов, требующих мониторинга, — это высококвалифицированные специалисты, обладающие знаниями в области высоконадёжных методов защиты информации. Именно они являются объектом интереса head-hunter-ов, в том числе по заказам международных террористических организаций.

Постоянных усилий требует также работа по согласованию взаимоприемлемых условий функционирования сети международных центров по предупреждению и противодействию кибератакам. Необходимо выработать работоспособные механизмы обмена опытом в этой области.

Документ как предмет и процесс

В. А. Конявский, В. А. Гадасин

Когда древние считали, что Земля плоская, это не мешало их жизнедеятельности. И только при переходе к длительным путешествиям, самолетам и ракетам, ошибочность предубеждения оказалась значимой.

В течение последних веков документы изготавливались с помощью традиционных технологий — раскраской цветными узорами (буквами и картинками) поверхности предмета (листа бумаги). И определение документа как «...зафиксированной на материальном носителе информации с реквизитами, позволяющими ее идентифицировать» [1, 2] было полезным. Но сейчас, с появлением электронного документа (ЭлД), применяемого в новых информационных технологиях, подобная трактовка становится неконструктивной.

Среди работ, посвященных данной тематике, можно выделить монографии [3–5]. В соответствии с [3], информация представляет собой результат отражения движения объектов материального мира в системах живой природы.

Информация обращается в коллективе однотипных организмов в *форме сведений* и *сообщений*. *Сведения* образуются в результате отражения организмами объектов материального мира, в том числе сообщений. *Сообщения* образуются организмами для передачи сведений другим организмам, содержат совокупность передаваемых сведений, и представляют собой набор знаков, с помощью которого сведения могут быть переданы другому организму и восприняты им. Этой позиции будем придерживаться и мы. Вопросы системных отличий традиционного и электронного документов, построения и изучения их моделей рассмотрены в [4].

В [5] прослежена эволюция определения термина «документ» за последние 30 лет.

В 70-х годах документ определялся [6] как «средство закрепления различным способом на специальном материале

информации о фактах, событиях, явлениях объективной действительности и мыслительной деятельности». В принятом в 1983 году ГОСТе [7] документ трактовался как «материальный объект с информацией, закрепленной созданным человеком способом для передачи ее во времени и пространстве». Определение [2] гласит, что документ — это «зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать».

В [5] эволюция определений оценивается как положительная, однако с этой оценкой трудно согласиться. Действительно, в первом определении конструкция «средство закрепления информации» неудачна, но, по крайней мере, определяется, какая информация (информация о чем) может быть сутью документа. Оказывается, далеко не любая, а только та, которая «закрепляет» «факты, события, явления объективной действительности и мыслительной деятельности»! Представляется, что эта часть определения в некоторой степени конструктивна, чего лишены другие определения. Многое ли для понимания сути документа (по существу, для таксономии «документ — не документ») может дать знание о том, что способ закрепления информации создан человеком? Искусственность происхождения имеет, видимо, отношение к признанию зафиксированного факта документом, но единственным признаком документа, как в [7], это быть вряд ли может.

Если же остановиться на определении из [2], то видно, что конструктивность из него исчезла полностью, включая и рукотворность. Согласно этому определению, документом можно признать и пустоты в пепле Помпеи, и следы на контрольно-следовой полосе, и даже окаменевшие остатки жизнедеятельности динозавров — если по ним можно установить хотя бы место и время этой жизнедеятельности.

Последовательность определений ярко иллюстрирует «вымывание» из них здравого смысла и конструктивности — мы наблюдаем эволюцию от «закрепленной» информации к «зафиксированной» информации. Закрепленность информации о фактах, событиях, явлениях — термин понятный и конструктивный, зафиксированность — просто неверный, глубоко ошибочный. Если мы говорим о «закреплении» — то возникающие вопросы касаются того, как «закрепить», посредством чего. Возникают схемы применения реквизитов и атрибутов, их защиты, структуры

и состава документа. Если мы говорим о «зафиксированности» информации, то единственным вопросом остается «на чем зафиксировано?». Как следствие, защита информации сводится к защите только носителя документа, со всеми вытекающими отсюда негативными последствиями.

Документ как материальный посредник информационного обмена

Рассмотрим определение Федерального закона «Об обязательном экземпляре документов» [8]: «*документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования*». Определение принято еще в эру безграничного господства документа на традиционном (бумажном) носителе, поэтому не будем обращать излишнее внимание на слова «материальный объект». Конечно, «...предназначенный для передачи во времени и пространстве в целях хранения...» — это промежуточная, подчиненная цель — не все ли равно, как документ будет транспортироваться, передаваться и/или храниться, лишь он был бы предъявлен «в нужном месте и в нужное время». Для нас важно, что основной функциональной целью документа является *общественное* использование.

Документ — явление социальное, присущее только общественной жизни мыслящих субъектов: в мире животных документа нет и быть не может, хотя обмен информацией имеется. Назначение документа — признаваемое обществом, т. е. *легитимное* (от лат. legitimus — согласный с законами, правомерный), объективно существующее формальное информационное основание для тех или иных действий участников информационного обмена.

В правовой сфере есть понятие [9] *юридический факт — предусмотренные в законе обстоятельства, при которых сохраняются или изменяются* (*возникают, прекращаются*) *конкретные правоотношения между участниками взаимодействия*. Возможность использования документа в качестве сообщения о юридическом факте в социальной среде обеспечивается обществом в лице государства. Высшая относительно любого из участников инстанция, используя свои институты

поощрения и наказания, предопределяет однозначную интерпретацию содержания, диктует реакцию участников на документ, предоставляет им права и налагает обязанности.

Однако юридический факт в рамках одного государства не является таковым в другом. Тем самым, говоря о документе, явно или неявно задается часть мирового общества, в данном случае — государство, в пределах которого он воспринимается адекватно.

Роль законов во фрагменте общества, члены которого объединены общими профессиональными, деловыми, или родственными интересами, играют неформальные, явные и неявные правила и обычаи, выработанные и «принятые к исполнению» *всеми* его членами. Здесь документ информирует уже не о *юридическом*, но просто о факте. Этот фрагмент общества (группу) будем называть *сектором действенности* документа.

Верно и обратное: сектор действенности — это такой фрагмент общества, в котором документ признается сообщением о факте (далее будем говорить — признается фактом).

Так как любой сектор действенности документа есть часть иерархически структурированного общества, то можно построить *иерархию* секторов, например, мир, государство, отрасль, фирма, знакомые, семья. Развивая иерархию, приходим к тому, что прямыми участниками электронного взаимодействия являются сектора из неодушевленных объектов. Правами и обязанностями эти объекты обладать не могут, но можно говорить о возможностях и ограничениях, накладываемых сектором действенности на свои компоненты. В электронном секторе правила (алгоритмы) трактовки ЭлД детерминированы, определяются обязательно вне рамок сектора, но точно также доводятся «до сведения» его членов, программно-технических объектов. Как и в социальной среде, эти возможности и ограничения относительно объектов сектора действенности ЭлД определяются «внешней силой». Но здесь эту роль играет субъект, ретранслирующий правила, установленные (техническом) обществом, и определяющий состав и конфигурацию инструментальных средств, программно-техническую базу, правила доступа, алгоритмы и дисциплину обработки, передачи и хранения ЭлД в системе.

Не уменьшая общности можно полагать, что *все* требования к документу формируются «напрямую» его сектором действенности. Таким образом, корректное задание документа означает

определение *пары*: {сообщение, закрепляющее факт; сектор действенности}.

Документ является сообщением о факте, которое признается в рамках сектора действенности легитимным основанием для сохранения, изменения, прекращения определенных взаимоотношений между членами сектора.

Функциональное назначение документа — его демонстрация

Необходимым и достаточным условием для того, чтобы документ исполнял роль сообщения о факте (служил информационным фактом), является его демонстрация по требованию сектора в заранее неопределенных моментах времени и точках пространства.

Чтобы обеспечить демонстрацию, документ должен быть реализован в материальной форме и предъявлен социуму в виде изделия. При этом он функционально служит лишь отправной точкой для различения порядка параметров. Система *чисел*-параметров данного изделия, считанная в определенном *порядке*, вполне «пригодна» для отображения информации, носителем которой это изделие является. Отображение рассматривается как упорядоченная совокупность (нематериальных) чисел — результатов физического измерения параметров изделия. Здесь мы сталкиваемся с понятием *порядка* для «информации».

Демонстрация документа — это предъявление в нужном месте и в нужный момент изделия-носителя информационного факта для того, чтобы с него были сняты ***предложенным сектором действенности*** *способом параметры — характеристики информации.*

Необходимо разделить два аспекта документа:

- нематериальный — правовой, признанное сектором действенности (группой) общества формальное основание определенных взаимоотношений;
- материальный — технологический, закрепленное созданным человеком способом отображение информации в виде изделия, которое может быть продемонстрировано группе как некоторый предмет или процесс.

Для окружающего нас мира только две материальные категории существования — *материя и энергия* — являются

базовыми. С математической точки зрения это равноправные категории описания реального мира, в том смысле, что одна не является следствием другой, в математике говорят — базисные аргументы.

И материя, и энергия материальны, измерение их параметров практически возможно — нет никаких оснований выбирать какую-то одну категорию в качестве приоритетной. Здесь возникает аналогия с предельными случаями: математическое описания сообщения $D(x,t)$. $D(x)$ — изделие-носитель расположено только в физическом пространстве X; $D(t)$ — сосредоточено только во временном пространстве T.

Это означает, что для отображения информации могут использоваться:

- пространственное изменение физических параметров *материи*, материального предмета, сосредоточенного в объеме *пространства* χ — традиционные технологии;
- временное изменение физических параметров *энергии*, материального сигнала, процесса, наблюдаемого в интервале *времени* τ — активные электронные технологии.

Таким образом, возможны два кардинально отличных вида изделий-носителей сообщения (документа): предмет и процесс. Соответственно — два направления защиты — традиционная защита носителя документа, и новое направление — защита информационных технологий как процессов обработки электронных документов.

Основным преимуществом предмета в качестве носителя документа является неизменность его параметров в течение длительного времени. Это свойство отвечает требованию *транспортировки во времени — хранения* документа. В активизированном состоянии (в режимах передачи, обработки электронного документа) сообщение существует в форме процесса. В этой форме эффективно решается проблема *транспортировки информации в пространстве*.

Вычислительная среда характеризуется обработкой и преобразованием информации на основе логических правил. Любой логический вывод есть совокупность последовательно выполняемых логических операций, поэтому множество, отображающее информацию, необходимо должно быть *последовательностью*. Не всякое множество есть последовательность, а только то, на котором задано отношение порядка.

Для ввода информации в вычислительную среду необходимо представить ее в виде *процесса* с фиксированной по времени очередностью характеристик. Активизированный электронный документ — это процесс (сигнал), электрические или электромагнитные характеристики которого изменяются во времени, их значения фиксированы во временной системе координат с началом отсчета, жестко связанным с началом активизации.

Отображение информации есть заданное сектором действенности и считанное в определенном ***порядке*** *множество* (*совокупность*) *физически измеримых параметров изделия-носителя*: *предмета*, *зафиксированного в пространстве*; *процесса*, *зафиксированного во времени*.

Отношение порядка на множестве должно быть «задано», а не «существовать». Должны быть известны признаки, позволяющие объектам электронной среды распознать это множество, для этого множество должно быть помечено, маркировано. Не требуется известность того субъекта или объекта, который задал отношение упорядоченности, важно только само отношение упорядоченности, которое должно «отслеживаться» программно-техническими объектами среды. Отображение информации — это маркированное детерминированным способом конечное множество, на котором задано бинарное отношение (частичной) упорядоченности: для любой пары элементов множества определено предшествование одного другому.

При информационном взаимодействии должно сохраняться отношение упорядоченности множества сигналов, *маркированного как «информация»*, *должен обеспечиваться* (*вычислимый*) ***изоморфизм*** *преобразований*.

Такой подход полностью совпадает с [10], где информация определяется как сущность, сохраняющаяся при (вычислимом) изоморфизме.

Математическая модель сообщения — пространство и время как категории отображения информации

И традиционное, и электронное сообщения используются для обеспечения взаимодействия субъектов экономики, так что их содержательное описание одинаково. Оба являются изделиями, пусть даже изготовленными по разным технологиям. Очевидно,

должна быть какая-то причина *системного* порядка для того, чтобы обусловить столь большую разницу в свойствах традиционного и электронного документа.

Из общей математической модели сообщения (документа) можно получить не совсем очевидные на практике следствия. Изделие-носитель D, находящееся в пространстве X и времени T, интерпретируется как некоторая многомерная функция $D(x,t)$, $x \in X$, $t \in T$, значений аргументов в окрестности $\chi \subset X$ точки пространства x и в интервале $\tau \subset T$ момента времени t. Формально аргументы x и t, χ и τ, X и T равноправны. Можно рассмотреть предельные случаи функции $D(x,t)$ и, если эти случаи «почти» совпадают с практическими феноменами, отождествить их с ними.

1. Изделие-носитель D сообщения от t не зависит. Отображение информации одинаково в любой момент времени, сосредоточено только в пространстве $\chi \subset X$ точки x, $D(x,t) = D(x)$, оно требует конечного объема χ пространства. Так как в состав аргументов время не входит, то интервал времени на съем информации лимитируется только средой существования изделия. В принципе достаточно «почти» нулевого времени, $\tau \approx O(0)$, восприятие информации одномоментное. Отображение считывается сканированием (порядок!) по пространству.

Примером такой пространственной категории является очень распространенный на практике носитель информации в форме предмета — твердого объекта с устойчивыми во времени, но изменяющими в пространстве характеристиками, отображающими собственно информацию. К этому же классу параметров относятся: рельеф поверхности носителя — азбука Брайля для слепых; грампластинка, CD-диск; различная намагниченность пленки; прозрачность предмета — кинопленка и др. Для электронного документа в пассивном состоянии магнитный носитель есть та же самая страница с буквами, где «буквы» отображены «раскраской» поверхности диска магнитными доменами с разной ориентацией.

Отображение информации параметрами предмета характеризуется конечным объемом пространства и, если пренебречь старением носителя, то бесконечным временем существования.

2. Изделие-носитель D сообщения от не зависит. Отображение информации присутствует во всех точках пространства X, но зато оно существует только во времени $\tau \subset T$ точки t, $D(x,t) =$

$D(t)$. Объем пространства на съем информации лимитируется только воспринимающим объектом, иначе в состав аргументов сообщения неминуемо входило бы пространство. В принципе достаточно «почти» нулевого пространства, $\chi \approx O(0)$. Отображение считывается сканированием (порядок!) во времени.

К этому классу принадлежит категория носителя информации в форме процесса: сигнала с изменяющими во времени, но устойчивыми в пространстве физическими характеристиками, отображающими собственно информацию.

При оплате покупки в современном магазине кассир считывает штрих-код товара специальным приспособлением, преобразующим его в запрос в базу данных о цене. В ответ на ЭлД-запрос компьютер выдает ЭлД-ответ, поступающий в кассовый аппарат. Контроллер кассового аппарата на основе ЭлД-ответа формирует ЭлД-чек на покупку, который преобразуется в бумажный аналоговый документ (АнД), чек с указанием даты, стоимости, сдачи, времени и пр. Ни один из промежуточных ЭлД не зафиксирован на носителе, каждый существует *только* как процесс. Да, цена покупки, время, номер кассы, наименование магазина где-то хранятся в памяти, но это всего лишь отдельные компоненты, но не ЭлД в целом. Иначе и азбуку можно рассматривать как «зафиксированную информацию» любого текстового документа.

Активный ЭлД принципиально должен отображаться в последовательном виде, так что время передачи конечно, в то же время — сигнал индицируется на контакте, а объем контакта (пространство) можно считать нулевым. ЭлД инвариантен к пространственным координатам, неточно локализован, сообщение одновременно присутствует в бесконечном числе точек пространства, либо не присутствует ни в одной точке.

Изготовление электронного документа для демонстрации

Кардинальное отличие новых информационных технологий от традиционных заключается в том, что они базируются на изготовлении сообщения (документа).

Не совсем корректно утверждение, что на экране монитора компьютера воспроизводится записанный на диске документ. Комплект технологической документации и комплектующие

на изготовление автомобиля и сама машина — это разные объекты. На диске записано информационное сырье — «полуфабрикаты», руководствуясь которыми на «станках» — элементах СВТ, создаются отдельные «детали» документа. Затем из «деталей» по «чертежам» — программному обеспечению, «собирается» готовое изделие — изображение на мониторе или распечатка на принтере.

Действительно, изготовление сообщения есть синтез двух составляющих — сырья и станка. На «вход» процесса-функции поступает сырье — числа-данные, на «выходе» появляются новые изготовленные числа-данные.

Заметим, что изготовление свойственно только электронному документу. При изготовлении исчезают все нюансы характеристик носителя аналогового документа в виде предмета, определяющих единственность, уникальность документа, его отличие от всех других «похожих». А как раз эти параметры позволяют индицировать искажение документа, гарантируют его подлинность, придают обычному информационному сообщению статус документа. Новые информационные технологии по самой своей сути не могут оперировать с интерпретацией оригинала как *единственного экземпляра* документа.

Содержание и атрибуты — переменная и постоянная части документа

Для того чтобы демонстрация изделия-документа выполняла функцию факта, необходимо требуется, чтобы *содержание* документа было неизменным, тождественным содержанию в момент создания. С другой стороны, сообщение, содержащееся в документе (будем говорить — закрепленное в нем), оставаясь постоянным для данного документа, для произвольного документа заранее неизвестно, и в этом смысле, случайно. Как же установить для произвольного документа, что закрепленное в нем сообщение осталось неизменным (т. е. убедиться в легитимности документа)? Возможен только один вариант — некоторые параметры, непосредственно связанные с отображением информации (содержанием) демонстрируемого изделия, должны быть неслучайны, «знакомы» членам сектора действенности. Сообщение произвольно, а значит, неслучайным может быть только оформление — атрибуты документа и технология преобразования,

передачи и хранения документа. Эта мысль частично отражена в нормативных определениях документа [1]: «...информация с *реквизитами*, позволяющими ее идентифицировать»; согласно [2], «реквизит документа — обязательный элемент оформления официального документа».

Естественно, не предполагается, что должны быть известны *все* характеристики исходного документа! Сектор действенности, предписывая технологию изготовления документа, задает ряд параметров, значения которых для демонстрируемого документа являются необходимым условием отсутствия искажений содержания.

Изделие-документ обязательно должно характеризоваться двумя группами параметров: основные, условно-переменные — отражающие содержание; и вспомогательные, условно-постоянные. Последнюю группу параметров будем называть атрибутами документа, включая в их состав и реквизиты документа как частный случай априорно заданных констант реализации документа в виде предмета или процесса. Таким образом, в состав документа-изделия непременно входит ряд эталонных (условно-постоянных) параметров. Только тогда, когда в выполнении этого требования сектор действенности *убежден*, возникают достаточные основания для признания сектором информации документированной, а сообщения — *документом*, (юридическим) фактом.

Задаваемые сектором действенности ***эталонные параметры*** *документа должны быть не только снимаемы с демонстрируемого изделия-документа, но и сравнимы* (*совпадают или нет*) *с параметрами эталона, т. е.* ***должны быть измеримыми***.

Свойства документа — доступность, целостность, легитимность

Теперь можно уточнить свойства, которыми должен обладать документ, имея в виду, что функциональное назначение документа — его демонстрация.

В точке демонстрации необходимо:

- измерить эталонные параметры предписанными сектором действенности средствами измерения;

- если отличие *всех* измеренных параметров от эталонных лежит в пределах, разрешенных сектором, присвоить изделию статус документа;
- в противном случае забраковать изделие.

Отсюда вытекают базисные требования к материальной реализации документа: доступность, целостность, легитимность.

Доступность *— физическая возможность измерения заданных параметров изделия-документа* (*содержания*, *атрибутов*, *технологии*) *предписанными сектором действенности средствами в заданных точках «пространство-время» в течение конечного времени с момента возникновения потребности в демонстрации.*

Так как технология измерения параметров задается сектором действенности, то время собственно измерения известно достаточно точно, и лимитирующим фактором является время доставки, перемещения документа к месту и моменту демонстрации. Передачу и хранение документа можно рассматривать в качестве вспомогательных процедур: не имеет значения, где и как хранится или передается документ, важна только возможность его демонстрации за конечное допустимое время с момента возникновения требования.

Целостность *— при любой демонстрации изделия-документа* ***эталонные*** *значения заданных сектором физических параметров демонстрируемого документа-изделия должны лежать в заданном допуске соответствующих параметров атрибутов документа в начальной точке жизненного цикла.*

Часто целостность трактуется как отсутствие искажений или изменений в документе в течение его жизненного цикла. Это не точно. Например, является ли искажением документа изменение его размеров при демонстрации на экране? Определение не должно базироваться на «отсутствии искажений» характеристик содержания — таких может быть бесконечно много, а должно опираться на «*наличие постоянства*» некоторых из них. Во-первых, установить наличие чего-нибудь проще, чем отсутствие; во-вторых, количество имеющихся признаков много меньше, чем отсутствующих.

Требование постоянства документа в течение жизненного цикла явно завышено — документ индицируется как факт только при

демонстрациях, суммарное время которых несопоставимо меньше жизненного цикла.

Легитимность (*лат. legitimus — законный*, *правомерный*) *— демонстрируемый изделие-документ должен содержать параметры, объективно подтверждающие правомерность использованных на протяжении жизненного цикла документа технологий.*

Приведем несколько примеров.

Закон как документ должен содержать объективные доказательства официальной публикации, поэтому разрозненные страницы, содержащие текст закона, не являются документом, даже если они вырваны, например, из «Собрания законодательства РФ». Текст доступен, целостен — но не легитимен. Демонстрируемый на экране видеофильм доступен и целостен, если имеются достаточные гарантии, что он не подвергался монтажу, и не использовались спецэффекты. Но статус документа видеофильм приобретет только тогда, когда есть уверенность, что проецирующая аппаратура не подменяет изображение. Секретная почта, доставленная посторонним прохожим, а не спецсвязью, вряд ли получит статус документа.

Часто сектор предписывает, например, подписать документ и поставить печать, причем образец подписи и печати необходимо предварительно зарегистрировать в третьем месте. Ясно, что регистрация есть составная часть технологии изготовления, хотя она и не имеет непосредственного отношения к данному документу.

Напомним — документ — это пара {сообщение, закрепляющее факт; сектор действенности}. Следовательно, требование к сообщению необходимо должно дополняться требованием к сектору. В данном случае, дополнительные требования выглядят следующим образом:

- *доступность* (параметров сообщения) — *конфиденциальность* (для подмножества субъектов сектора);
- *целостность* (параметров сообщения) — *инвариантность* (других параметров с точки зрения сектора);
- *легитимность* (применяемых технологий) — *вариабельность* (других технологий с точки зрения сектора).

Как пример, рассмотрим дополнительное требование конфиденциальности. Сектор действенности требует, чтобы определенные

параметры документа (текст) не могли бы наблюдаться заданным кругом субъектов или объектов (например, конкурентами), были бы им недоступны. Но это элементы того же самого сектора действенности, в котором документ должен быть доступен согласно первому базисному требованию. Значит, должно быть определено ограничение, относящееся не непосредственно к документу, а к субъектам сектора, существующим вне зависимости от документа. Например, технология демонстрации предполагает дифференциацию субъектов сектора по допуску. Или только выделенная группа субъектов обладает средствами индикации (измерения) «смысла» документа — алгоритмами (ключами) шифрования и расшифрования.

Защита информационных технологий

Электронный документ существует в виде *предмета* в аналоговой среде и в виде *процесса* в цифровой (электронной) среде. Отличие процесса и объекта имеет системный характер, поэтому в защите электронного информационного обмена выделяются два качественно разных направления: защита предмета, т. е. собственно отображения информации; защита процессов преобразования — технологий, *инвариантных* к защищаемой информации. Первое направление характерно для статической формы представления информации физическими свойствами объекта. Информация *фиксируется* параметрами предмета, которые необходимо должны быть постоянны в течение жизненного цикла документа, причем доступ к их измерению (наблюдению) ограничивается. В этом случае говорят о *защите информации*, понимая защиту предмета-носителя от несанкционированного доступа. Такая форма представления информации *доминирует* в аналоговой среде существования документа, хотя имеет место и в электронной среде, например, в случае хранения ЭлД в устройствах памяти.

Методы защиты зафиксированной аналоговой информации, *информации-предмета*, отработаны теорией и практикой применения традиционных аналоговых документов. С этих позиций *защита электронного документа в аналоговой форме существования* не имеет существенных особенностей по сравнению с традиционными аналоговыми документами и поэтому далее не рассматривается.

Содержанием комплекса мероприятий, понимаемых как защита ЭлД-процесса, является *не защита информации*, *а защита допустимости технологии*, применяемой при физической реализации документа в виде объекта или процесса.

Основное требование к защите информации — сохранение отношения упорядоченности знаков, символов (изоморфности). Основное требование к защите технологии — сохранение отношения упорядоченности отдельных операций, ее составляющих. Соответственно, нуждается в уточнении определение информационной технологии. Если ранее [11] информационная технология понималась как: «Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных», то точнее будет дополнить это определение словом «последовательность», что бы подчеркнуть, что технология — это не «совокупность» применяемых в произвольной последовательности «приемов». Таким образом, «информационная технология — это *последовательность* приемов, способов и методов применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных».

Таким образом, в процессе изготовления ЭлД участвуют такие объекты, как:

- компьютеры,
- данные (другие ЭлД),
- сетевые (телекоммуникационные) средства,
- и *информационные технологии*.

В соответствии с этим, в мероприятиях по технической защите можно выделить:

1) аутентификацию участников информационного взаимодействия,
2) защиту технических средств от НСД,
3) разграничение доступа к документам, ресурсам ПЭВМ и сети,
4) защиту электронных документов,
5) защиту данных в каналах связи,
6) защиту информационных технологий,
7) разграничение доступа к потокам данных.

Заметим, что пункты 1, 2, 3, 5 и отчасти 7 в совокупности и составляют предмет традиционно понимаемой «защиты информации». Очевидно, что реально предмет гораздо шире, есть еще,

по крайней мере, пункты 4 и 6. Этим вполне можно объяснить отсутствие значимых успехов в традиционных подходах к решению практических задач.

Литература

[1] Федеральный закон «Об информации, информатизации и защите информации» (от 20.02.1995 г.) // СЗ РФ. 1995. № 8. Ст. 609.

[2] ГОСТ Р 51141-98. «Делопроизводство и архивное дело. Термины и определения». М., 1998.

[3] *Стрельцов А. А.* Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В. А. Садовничего, В. П. Шерстюка. М., 2002.

[4] *Гадасин В. А.*, *Конявский В. А.* От документа — к электронному документу. Системные основы. М., 2001.

[5] Информационные ресурсы развития Российской Федерации: Правовые проблемы / Ин-т государства и права. — М.: Наука, 2003.

[6] ГОСТ 16487-70. «Делопроизводство и архивное дело. Термины и определения». М., 1971.

[7] ГОСТ 16487-83. «Делопроизводство и архивное дело. Термины и определения». М., 1983.

[8] Федеральный закон «Об обязательном экземпляре документов» (от 29.12.1994 г.) // СЗ РФ. 1995. № 1. Ст. 1.

[9] Большой юридический словарь / Под ред. А. Я. Сухарева, В. Е. Крутских. М., 2000.

[10] *Кузнецов Н. А.*, *Мусхелишвили Н. Л.*, *Шрейдер Ю. А.* Информационное взаимодействие как объект научного исследования (перспективы информатики). — Вопросы философии, № 1, 1999, с. 77–87.

[11] ГОСТ 34.003-90 «Информационные технологии. Комплекс стандартов и руководящих документов на автоматизированные системы». М., 1990.

Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы)

А. П. Коваленко, Е. Б. Белов

Новое столетие характеризуется стремительным развитием телекоммуникационных и информационных технологий, которые радикально изменили нашу жизнь и становятся одним из доминирующих факторов в формировании общества XXI века. При этом принципиальное значение приобретают вопросы обеспечения информационной безопасности, разработки таких технологий защиты информации, которые бы обеспечили динамичное и равноправное вхождение России в мировое информационное сообщество.

Подготовка специалистов с высшим образованием в области информационной безопасности (ИБ) в стране имеет более чем 50-летнюю историю, если вести отсчет со времени начала подготовки в стране криптографов на базе закрытого отделения Механико-математического факультета МГУ им. М. В. Ломоносова. Однако как система такая подготовка стала складываться только в начале 90-х годов благодаря развитию новых информационных и телекоммуникационных технологий.

В настоящее время Минобразованием России совместно с заинтересованными федеральными органами исполнительной власти создана основа государственной системы подготовки специалистов с высшим профессиональным образованием, способных решать задачи обеспечения ИБ страны прежде всего в их естественнонаучной и технической составляющих. Эта система включает в себя:

- Учебно-методическое объединение вузов Росси по образованию в области ИБ на базе Института криптографии,

связи и информации Академии ФСБ России (УМО ИБ) и Учебно-методический совет Российского государственного гуманитарного университета (УМС РГГУ).

- Группу государственных образовательных стандартов высшего профессионального образования (ГОС ВПО) 075000 «Информационная безопасность», включающую семь специальностей: «Криптография», «Компьютерная безопасность», «Организация и технология защиты информации», «Комплексная защита объектов информатизации», «Комплексное обеспечение информационной безопасности автоматизированных систем», «Информационная безопасность телекоммуникационных систем», «Противодействие техническим разведкам».
- Образовательные программы (программы специальностей, магистерские программы, программы специализаций), смежные с входящими в группу 075000, реализуемые в рамках других УМО.
- Образовательные программы дополнительного и послевузовского профессионального образования (подготовка кадров высшей квалификации) в области ИБ, включая специальность 05.13.19 «Методы и системы защиты информации. Информационная безопасность».
- Более 100 вузов России различной ведомственной принадлежности, которые осуществляют подготовку специалистов по указанным специальностям.
- 12 министерств и ведомств и их органов управления профессиональным образованием, а также научные организации и учреждения, ведущие научные исследования в данной области, в том числе два головных центра — МГУ им. М. В. Ломоносова и Академия криптографии РФ.
- 25 региональных учебно-научных центров по проблемам ИБ в системе высшей школы с головным центром на базе МИФИ.
- Различные ведомственные курсы переподготовки и повышения квалификации.

Высокие темпы формирования этой системы в естественнонаучном и техническом направлениях объясняются, на наш взгляд, наличием сложившейся основы подготовки в вузах силовых структур, большой наукоемкостью специальностей, высоким спросом на специалистов на рынке труда, адаптированностью

содержания образования к традициям технических вузов и математических факультетов классических университетов. Структура системы подготовки кадров в области ИБ представлена на рис .

Следует отметить, что в системе ФСБ, Минобороны, ФСО, МВД, Гостехкомиссии, МПС России, других министерств и ведомств действуют подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Минобразовании России. Данные подсистемы нацелены на подготовку кадров в интересах конкретных ведомств и поэтому имеют определенную специфику как по своей организации и содержанию, так и по направлениям развития.

Коренные изменения государственной политики Российской Федерации в области национальной безопасности, в частности информационной безопасности, в области образования и информатизации, накопленный опыт создания и функционирование системы подготовки кадров в области обеспечения информационной безопасности, результаты анализа ее состояния определяют актуальность разработки Концепции подготовки кадров в области информационной безопасности (далее — Концепция).

Концепция должна представлять собой систему положений, определяющих основные задачи, принципы, направления совершенствования, первоочередные мероприятия и ожидаемые результаты развития системы подготовки кадров в области информационной безопасности в Российской Федерации. Она должна создать методологическую основу для согласования деятельности всех субъектов законодательной инициативы, федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, образовательных учреждений, научных организаций, государственно-общественных и общественных объединений, потребителей специалистов, действующих в рассматриваемой области.

Положения Концепции должны опираться на Конституцию Российской Федерации, Послания Президента Российской Федерации Федеральному Собранию Российской Федерации, Федеральные законы «Об информации, информатизации и защите информации», «О средствах массовой информации», «Об участии в международном информационном обмене», «О связи», «О государственной поддержке средств массовой информации и книгоиздания в Российской Федерации», «О государственной тайне», Федеральные законы в сфере образования,

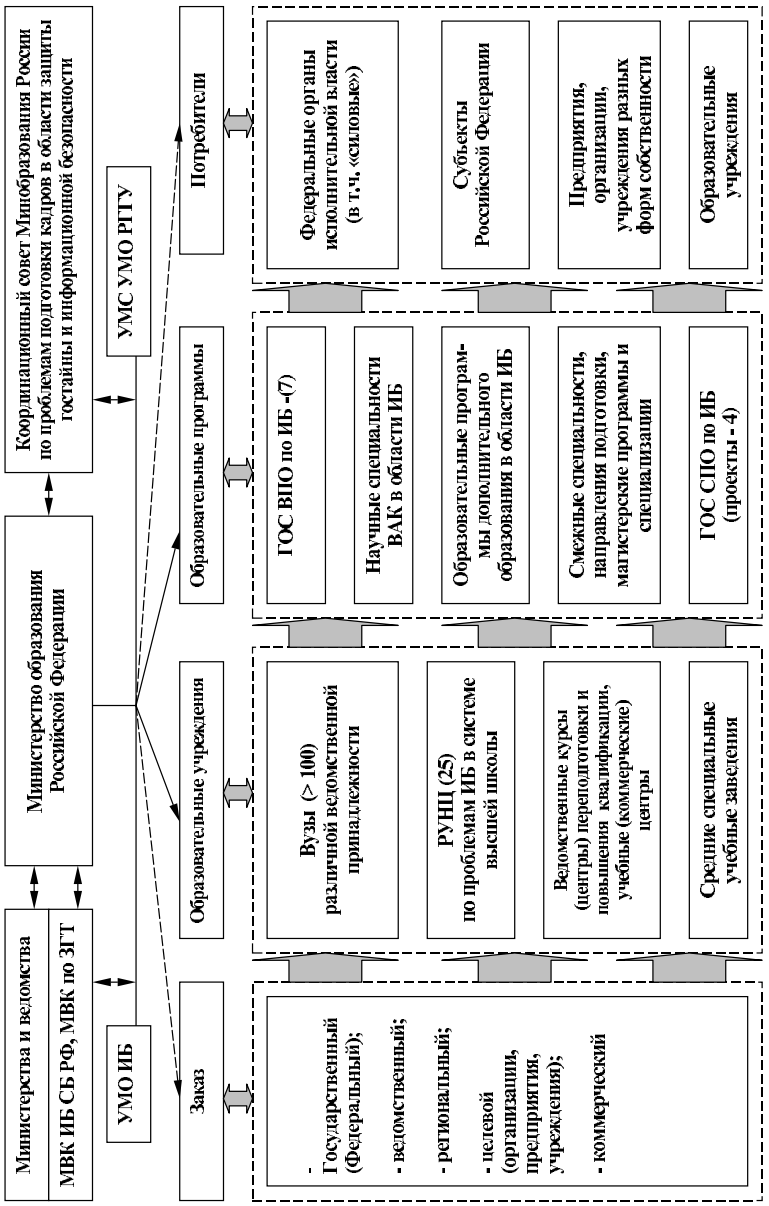

Рис. 1. Структура системы подготовки кадров в области информационной безопасности.

Концепцию национальной безопасности Российской Федерации, Доктрину информационной безопасности, Концепцию защиты государственной тайны, Концепцию модернизации Российского образования на период до 2010 года, Национальную доктрину образования в Российской Федерации до 2025 года, Федеральную программу развития образования на 2000–2005 годы, Концепцию управления государственными информационными ресурсами, Концепцию государственного регулирования негосударственными информационными ресурсами, Федеральную целевую программу «Электронная Россия 2002–2010», Федеральную целевую программу «Развитие единой образовательной информационной среды (2001–2005 годы)», нормативные правовые документы Правительства Российской Федерации о формировании государственного плана подготовки инженерных и научных кадров для организаций оборонных отраслей промышленности на 2002–2005 годы и о конкурсном порядке размещения государственного задания на подготовку специалистов с высшим профессиональным образованием (образовательная область — информационная безопасность), ведомственные концепции в области информатизации, решения Межведомственной комиссии по защите государственной тайны и Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности, а также на разрабатываемые Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации, государственной информационной политики, иные законодательные акты, регулирующие отношения субъектов в информационной сфере, выводы отечественных и зарубежных ученых по проблемам построения информационного общества и формирования информационно-телекоммуникационного пространства, результаты аналитических и прогнозных исследований процессов информатизации в России.

Доктрина информационной безопасности Российской Федерации (далее — Доктрина) определяет значение информационной безопасности как составляющей национальной безопасности страны следующим образом: национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать. Поэтому профессиональная подготовка, переподготовка и повышение квалификации

кадров в данной области выступает как важная составляющая в комплексе мероприятий по противодействию угрозам жизненно важным интересам государства в информационной сфере.

Особенности содержания подготовки кадров в области информационной безопасности и требований, предъявляемых к образовательным учреждениям, реализующим такую подготовку, определяются принципами подготовки кадров в области ИБ, к числу которых следует отнести:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации в области национальной безопасности и образования;
- гармоничное сочетание интересов личности, общества и государства;
- рациональное определение числа вузов, осуществляющих подготовку специалистов в области ИБ;
- тщательный подбор кадров (обучаемых и профессорско-преподавательского состава);
- целевая государственная поддержка ведущих вузов страны, научно-педагогических коллективов, осуществляющих подготовку специалистов в области ИБ для министерств и ведомств Российской Федерации;
- обоснованное сочетание открытых и закрытых специальностей в области ИБ;
- гармоничное развитие специальностей и содержания образовательных программ в различных областях наук, включая естественнонаучные, технические и гуманитарные;
- единство системы подготовки кадров в области информационной безопасности с учетом совокупности программно-аппаратных, криптографических, технических, информационно-психологических, организационных и правовых методов защиты информации;
- принцип сопряженности образовательных траекторий и образовательных программ в области ИБ.

Реализация этих принципов позволит, на наш взгляд, наметить правильные пути совершенствования системы подготовки кадров в области ИБ.

В Доктрине констатируется тот факт, что проблемы ИБ перестали сегодня быть областью исключительной компетенции специальных служб (государства), они все больше становятся

предметом внимания общества и личности. Объясняется это следующими обстоятельствами:

1. Информация все больше становится таким атрибутом, от которого в решающей степени зависит эффективность жизнедеятельности всех сфер современного общества.
2. Происходящие в последние годы в стране изменения, переход к более открытому обществу, создают в то же время благоприятную обстановку для несанкционированного доступа к информации, в том числе конфиденциальной.
3. Всеобщая компьютеризация основных сфер деятельности привела к появлению широкого спектра нетрадиционных каналов утечки информации и несанкционированного доступа к ней.

Последнее обстоятельство таит в себе реальную угрозу несанкционированного контроля над информационными процессами. Это особо опасно в связи с тем, что программно-техническая база информатизации в России практически целиком основана на продукции зарубежных фирм. В то же время развитие информационных технологий уже в недалеком будущем способно привести к появлению качественно новых форм борьбы, так называемых информационных войн. Учитывая это, Государственный комитет Российской Федерации по высшему образованию еще в 1992 г. сформировал специальную межвузовскую программу и организовал проведение силами вузовских ученых комплексных исследований всей совокупности проблем, связанных с обеспечением безопасности информации.

Первый вывод из полученных результатов сводится к тому, что проблемы обеспечения информационной безопасности будут носить перманентный характер, они не могут быть решены путем разовой реализации какого-либо проекта. Отсюда следует, что в России должна быть создана развитая и регулярно функционирующая система, способная своевременно и эффективно решать всю совокупность возникающих в этой области задач.

Второй вывод состоит в том, что обеспечение информационной безопасности в современных условиях должно носить комплексный характер, причем как по целям, так и по способам и используемым средствам. Принципиальное значение имеет то, что в современных условиях информационная безопасность не может быть сведена к ставшей уже традиционной защите информации. Важнейшей составляющей информационной безопасности

становится защита от информации, заключающаяся в предупреждении от разрушающего воздействия информации на электронные средства, системы и на людей (отдельно взятого человека, коллектив, общество). Необходимо иметь в виду, что защита от деструктивного информационного воздействия становится все более актуальной проблемой.

Третий вывод заключается в том, что обеспечение комплексной безопасности информации не может быть достигнуто лишь усилиями специалистов-профессионалов в области ИБ. Необходимо непосредственное и активное участие тех руководителей и специалистов, которые организуют и осуществляют процессы сбора, передачи, хранения, обработки и использования информации.

Четвертый вывод, который сформулирован по результатам исследований, сводится к тому, что рассматриваемые проблемы должны решаться в тесной взаимосвязи с проблемами законодательно-правового регулирования процесса информатизации. Это создает необходимое правовое пространство, которое способствует повышению эффективности обеспечения информационной безопасности.

Наконец, пятый вывод заключается в том, что эффективное решение проблем информационной безопасности на научной основе требует высокоорганизованного кадрового обеспечения, то есть регулярной подготовки, переподготовки и повышения квалификации необходимого числа специалистов, обладающих соответствующим объемом и уровнем знаний и навыков.

Минобразования России совместно с заинтересованными федеральными органами исполнительной власти провело работу, в результате которой к настоящему времени в основном сформирована организационная и методическая база для подготовки специалистов.

Приказом Министра образования РФ от 25.02.2003 № 670 создан Координационный совет Минобразования России по проблемам подготовки кадров в области защиты государственной тайны и информационной безопасности, в который вошли представители заинтересованных министерств и ведомств. Создана группа специальностей 075000 «Информационная безопасность», по которым разработаны и утверждены Минобразованием государственные образовательные стандарты высшего профессионального образования, примерные учебные

планы и примерные программы дисциплин, требования к учебно-методическому и материально-техническому обеспечению. Сформирована электронная база данных обеспеченности ГОС по специальностям в области ИБ учебно-методическими изданиями. Разработаны и изданы учебники и учебные пособия по основным дисциплинам.

Если вернуться к истории вопроса, то следует отметить, что формирование новой группы специальностей в области ИБ проходило достаточно сложно, несмотря на поддержку ряда ведомств. Решающее значение в этом процессе сыграло обращение ректора МГУ им. М. В. Ломоносова академика В. А. Садовничего в адрес Минобразования России о необходимости создания такой группы специальностей.

Утвержден «Федеральный компонент по основам информационной безопасности и защиты государственной тайны в Государственных образовательных стандартах» и перечень специальностей, на которые распространяется данный Федеральный компонент. В рамках дополнительного профессионального образования разработаны типовые программы повышения квалификации по вопросам информационной безопасности и защиты государственной тайны для различных категорий специалистов (руководителей предприятий, сотрудников подразделений, обеспечивающих информационную безопасность, специалистов по эксплуатации современных информационно-вычислительных систем), однако пока не создана система их внедрения. По нашему мнению, необходимо организовать реализацию типовых программ повышения квалификации и переподготовки специалистов различного профиля и уровня с привлечением УМО ИБ.

В системе послевузовского образования сформирована научная специальность 05.13.19 «Методы и системы защиты информации. Информационная безопасность». Действует 9 кандидатских и 12 докторских советов.

В среде образовательных учреждений интенсивно ведется обмен опытом — ежегодно проводится до десяти общероссийских конференций и иных мероприятий по тематике информационной безопасности и защиты информации, где рассматриваются и вопросы подготовки кадров.

К настоящему времени количество вузов, начавших подготовку специалистов по специальностям данной группы, уже превысило отметку 100. Распределение вузов по специальностям

приведено в таблице 1. Общее методическое руководство развитием специальностей группы осуществляют учебно-методические объединения (головные вузы — Институт криптографии, связи и информатики Академии ФСБ России и Российский государственный гуманитарный университет).

Индекс	**Наименование специальности**	**Число лицензированных вузов**
075100	Криптография	1
075200	Компьютерная безопасность	27
075300	Организация и технология защиты информации	44
075400	Комплексная защита объектов информатизации	24
075500	Комплексное обеспечение информационной безопасности автоматизированных систем	30
075600	Информационная безопасность телекоммуникационных систем	11
075700	Противодействие техническим средствам разведки (экспериментально)	1

Таблица 1. Перечень специальностей ВПО в области ИБ.

Подготовкой специалистов охвачены практически все регионы России.

Опыт реализации данных специальностей, а также запросы практики показали необходимость решения в ближайшей перспективе следующего комплекса основных проблем:

1. По-прежнему актуальна проблема развития системы подготовки кадров в области информационной безопасности как по «вертикали» — с охватом всех уровней подготовки, так и по «горизонтали» — с выходом на проблемы информационной безопасности в гуманитарной сфере и на стыке естественнонаучных, технических и гуманитарных направлений. В первую очередь

это относится к подготовке и переподготовке специалистов правоохранительных органов, органов суда и прокуратуры в области борьбы с преступлениями в сфере компьютерной информации. Представляется необходимым создать систему непрерывного профессионального образования специалиста в области ИБ.

2. Потребности общества и государства в специалистах с высшим профессиональным образованием в области ИБ удовлетворяются не в полной мере. По данным Минобразования России на 2002 год прием студентов по группе специальностей 075000 составил: 1500 чел. — на бюджетные места, около 1000 чел. — на платные места. Прогнозируемая потребность в специалистах на 2003–2006 гг. составляет 5000 человек ежегодно, контрольные цифры приема определены в объеме 2000 студентов. Хотя абсолютные цифры набора по данной группе специальностей значительно уступают другим группам, увеличение контрольных цифр приема по сравнению с 2002 годом предусмотрено в объеме 30–55%, что почти на порядок превышает все остальные группы специальностей. При этом не исследованы потребности негосударственного сектора, роль которого в экономике страны постоянно возрастает. К тому же и сам механизм определения потребностей в специалистах в области обеспечения информационной безопасности требует совершенствования.

3. За последние годы изменилась нормативная правовая база обеспечения информационной безопасности. Расширился круг задач, решаемых в области в данной области. В частности, это относится к вопросам защиты конфиденциальной информации, использования электронной цифровой подписи и др. Это требует уточнения реестра должностей специалистов, техников и служащих, а также и их обязанностей.

4. Зачастую специалисты с высшим образованием вынуждены выполнять техническую работу, так как отсутствует подготовка специалистов со средним профессиональным образованием.

5. Инспекторские проверки соответствующих федеральных органов исполнительной власти выявили недостаточный уровень квалификации специалистов по обеспечению информационной безопасности критически важных объектов информационной инфраструктуры Российской Федерации. Следует отметить, что проблема повышения качества подготовки специалистов для федеральных органов власти предполагает решение целого

комплекса вопросов, включающих определение готовности образовательного учреждения к реализации соответствующих программ, мониторинг качества подготовки в процессе обучения, поддержание на требуемом уровне материально-технической базы, подготовку научно-педагогических кадров.

6. Масштабы подготовки и переподготовки специалистов по проблемам информационной безопасности в системе Минобразования еще недостаточно подкреплены в ресурсном отношении. Специализированная материально-техническая и лабораторная база в большинстве вузов пока не удовлетворяет современным требованиям. Кроме того, в ряде образовательных учреждениях не обеспечен необходимый уровень преподавательских кадров высшей квалификации.

* * *

Для решения указанных проблем к настоящему времени Минобразованием России с привлечением заинтересованных федеральных органов исполнительной власти, УМО ИБ и УМС РГГУ проведен ряд мероприятий. Так, в рамках Федеральной программы развития образования выполнена НИР на тему «Разработка сопряженных профессионально-образовательных программ в области информационной безопасности». В результате были разработаны проекты двух стандартов по направлению бакалавр-магистр, проекты четырех стандартов среднего профессионального образования, восемь образовательных программ по специализациям в рамках гуманитарных специальностей (три по специальности «Юриспруденция», четыре по специальности «Психология», одна по специальности «Экономика и управление на предприятии»). Также разработаны три образовательные программы по специализациям в рамках смежных технических специальностей и два проекта программ для присвоения дополнительной квалификации. Нормативное закрепление результатов данной НИР позволит существенно расширить границы образовательных траекторий подготовки кадров в области ИБ.

На базе ИКСИ Академии ФСБ России организованы курсы по повышению квалификации преподавателей вузов, реализующих специальности в области ИБ.

Минобразования России ежегодно выделяет средства на проведение научно-исследовательских работ для методического обеспечения подготовки кадров в области информационной

безопасности. В то же время, как по объему финансирования, так и по организации совместных работ с другими заинтересованными структурами возможности Минобразования недостаточны для радикального решения многих задач. Это требует привлечения ресурсных возможностей других заинтересованных министерств и ведомств, субъектов негосударственного сектора экономики, а также предприятий и организаций различных форм собственности.

Для решения перечисленных выше проблем, по нашему мнению, актуальными являются следующие направления деятельности:

- Усиление координации всех звеньев образовательной системы, потребителей специалистов и силовых структур, ответственных за обеспечение информационной безопасности с целью уточнения прогноза количества и квалификации специалистов, необходимых для решения проблем обеспечения информационной безопасности России. Необходимо разработать новую редакцию квалификационных характеристик должностей руководителей, специалистов и служащих, занятых на предприятиях, в учреждениях и организациях в области обеспечения ИБ в соответствии с действующими нормативными правовыми актами, согласовать требования государственных образовательных стандартов высшего и среднего, профессионального образования, а также соответствующие требования послевузовского и дополнительного образования с действующими и уточненными квалификационными характеристиками;
- Расширение комплекса образовательных программ по проблемам ИБ в направлении среднего профессионального образования, специализаций правового, управленческого, экономического, социального и технического характера, внедрение этих программ.
- Формирование в системе Минобразования, а также в заинтересованных министерствах и ведомствах целенаправленной подсистемы повышения квалификации и переподготовки по проблемам ИБ руководителей и сотрудников самых разнообразных уровней как государственных организаций, так и предприятий различных форм собственности.

Несмотря на оптимистическую картину развития подготовки специалистов по группе специальностей 075000 «Информационная безопасность», вызывает сомнение качество подготовки, достигаемое при столь стремительном расширении направлений подготовки в вузах, ранее ими не занимавшихся. Необходимо провести анализ состояния подготовки в вузах, открывших данные специальности и принять меры по обеспечению необходимого качества подготовки специалистов этой группы во всех регионах России, уделив особое внимание развитию механизмов лицензирования, аттестации и аккредитации образовательных учреждений, укреплению их материально-технической базы, расширению подготовки и переподготовки преподавателей высшей квалификации. Проблемы кадрового обеспечения в сфере информационной безопасности требуют своего обсуждения на Коллегии Минобразования России.

В рамках научно-исследовательских программ Минобразования России ИКСИ Академии ФСБ России, МГТУ им. Н. Э. Баумана в 2002 году был разработан проект Концепции подготовки кадров в области информационной безопасности. По нашему мнению, данную работу необходимо продолжить под руководством Минобразования с привлечением федеральных органов исполнительной власти и довести ее до практической реализации в виде Федеральной (межведомственной) программы развития образования в области информационной безопасности.

Литература

[1] *Белов Е. Б.* О подходах к разработке концепции подготовки кадров в области информационной безопасности // Информация и безопасность. Материалы межрегиональной научно-практической конференции «Информация и безопасность» Воронеж: Воронежский ГТУ, 2002. Вып. 2. С. 35–38.

[2] *Белов Е. Б.*, *Лось В. П.* Образование в области информационной безопасности: принципы совершенствования системы подготовки кадров // Информационное право: информационная культура и информационная безопасность. Материалы Всероссийской научно-практической конференции. 17–19 октября 2002 г. СПб.: Изд-во СПбГУП, 2002. С. 123–124.

[3] *Белов Е. Б.*, *Кравченко В. Б.*, *Крекотень С. П.* Развитие структуры полготовки кадров для деятельности в области информационной безопасности // Материалы III межведомственной научно-технической конференции Краснодарского военного института 17–18 сентября 2002 г. Том 1. Краснодар.: КВИ, 2002. С. 7–13.

[4] *Коваленко А. П.*, *Лось В. П.*, *Смирнов С. Н.* Проблемы подготовки специалистов в сфере информационной безопасности в московском регионе // Сборник материалов летней сессии «Инфофорума-5» — 5-й Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества». М.: Редакция журнала «Бизнес + Безопасность», 2003. С. 85–88.

[5] *Стрельцов А. А.* Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В. А. Садовничего и В. П. Шерстюка. М.: МЦНМО, 2002.

[6] *Голованов П. Н.* Влияние выпускников Московского университета на становление криптографического образования в России // Московский университет и развитие криптографии в России. М.: МЦНМО, 2002, с. 258–270.

[7] 50 лет Институту криптографии, связи и информатики (исторический очерк). М., 1999.

[8] *Коваленко А. П.*, *Смирнов С. Н.* Организация образования в области информационной безопасности в России / Информационные системы и технологии (IST'2002): Материалы I Международной конф. (Минск, 5–8 ноября 2002 г.): В 2 ч. Ч. 2. — Минск: БГУ, 2002. С. 56–61.

[9] Материалы заседаний межведомственного междисциплинарного семинара по научным проблемам информационной безопасности (за период 2000–2003 гг.). Руководители: Садовничий В. А., Сачков В. Н., Шерстюк В. П. М.: Изд-во МГУ.

Экономика информационной безопасности. Предметная область и постановка проблемы

М. И. Лугачёв, С. Н. Смирнов

Общество, в которое мы живем, часто называют «информационным обществом». Действительно, трудно представить современную цивилизацию без вычислительных машин и телекоммуникаций, без автоматизированных систем и информационных технологий. Средства массовой информации являются одной из наиболее мощных сил, формирующих направление развития цивилизации. Фирмы информационной индустрии существенно потеснили традиционных промышленных гигантов в мировых рейтингах как по обороту капитала, так и по доходам. Даже в списке обладателей наибольшего личного состояния в верхних строчках присутствуют представители информационной индустрии: Билл Гейтс, Стив Баллмер (Microsoft), Ларри Эллисон (Oracle).

В информационной сфере занята значительная часть современного общества. Естественно, что экономические отношения, возникающие между людьми и организациями, в процессе их деятельности в информационной сфере должны быть осмыслены на уровне научного познания. Информационную сферу можно представить как совокупность информационных ресурсов, информационной инфраструктуры, системы формирования, распространения, использования информации и регулирования возникающих при этом общественных отношений. Информационная сфера является системообразующим фактором жизни общества, активно влияет на состояние политической, экономической и других составляющих безопасности государства.

Информация, как предмет экономического анализа

В современной экономической деятельности информация служит таким же ресурсом, как труд и капитал. Чтобы приобрести

такое высокое положение в экономике, понадобились долгие годы, в течение которых взгляд на информацию или концепция ее роли в обеспечении функционирования субъектов экономической деятельности заметно трансформировалась.

Переход к информационному обществу существенно меняет роль материальных факторов в развитии современного мира. Если в традиционном обществе главное место занимали процессы производства и распределения материальных благ, а также отношения, возникающие в ходе этих процессов, то в информационном обществе на первое место выходят информационные процессы — процессы сбора, хранения, обработки и представления информации. Информационные процессы касаются данных, собственно информации и знаний. Сегодня наблюдается достаточно конкретных примеров того, что материальные составляющие в структуре жизненных благ постепенно уступают приоритеты информационным.

Чем же отличается информация от материальных продуктов? Обратимся к мнению профессора Е. Э. Майминаса по этому поводу: «Главным, коренным отличием является ее неуничтожаемость в процессе потребления (использования), возможность многократного потребления и не одним, а многими потребителями (пользователями)». Информацию не теряет, не лишается ее производитель — в процессе передачи потребителю она сохраняется и у производителя. Некоторая схожесть с основными фондами остается кажущейся, внешней: основные фонды «расходуются», изнашиваются в процессе их потребления-использования, а информация — нет, хотя и она стареет и обесценивается со временем.

Кроме того, с экономической точки зрения информация имеет такие особенности, как трудность определения потребителя при массовом распространении и трудность определения точной стоимостной оценки полученной информации. Эти особенности определяют специфику соответствующего рынка. На информационном рынке, как и на всяком другом, товар стоит столько, сколько за него платят. Но существует и успешно развивается рынок контрафактной, нелицензионной продукции, где такие информационные товары как программное обеспечение, компьютерные игры, фильмы, музыкальные произведения стоят гораздо меньше, чем на официальном информационном рынке. Информация является товаром особого рода.

Информация как стратегический ресурс субъекта экономической деятельности

Предпринимательское восприятие информации радикально изменилось в сторону признания ее стратегического значения для функционирования организации в начале 90-х годов XX века. Широкое распространение персональных компьютеров, локальных вычислительных сетей, становление всемирной сети Интернет превратили информацию в существенный фактор технологий производства продукции и услуг. Господствовавшая много десятилетий концепция повышения производительности сменилась концепцией высокой эффективности. Концепция повышения производительности требовала повышения выпуска продукции в единицу времени при заданном уровне качества (например, с помощью конвейерной системы Форда). Производительность, как главная концепция организации производства, отвечала на вопрос: «*Как* производить?».

Развитие информационных процессов превратило производительность в необходимый, но не достаточный фактор в борьбе с конкурентами. На первый план вышла борьба за потребителя продуктов и услуг. Главным вопросом стал вопрос «ЧТО производить?». Важнейшим фактором обеспечения конкурентоспособности предприятия стала борьба за потребителя. Продукт или услуга должны быть не только произведены «как надо», но и достаточно быстро потреблены. Только в этом случае производство становилось эффективным, а предприятие конкурентоспособным.

Для ответа на вопрос «что производить?» необходимо было собрать и обработать огромные массивы информации по различным категориям:

- о материалах (с целью быстрейшего внедрения появляющихся новых материалов, которые могут быть использованы для производства продукции в будущем);
- о технологиях (с целью использовать передовые и эффективные технологии в собственной деятельности, включая и информационные технологии);
- об управлении (с целью реализации наиболее эффективных схем управления, в том числе с использованием современных информационных систем);
- о конкурентах;

- о нормативном регулировании экономической деятельности;
- о состоянии финансового рынка;
- о клиентах.

Последняя позиция в этом неполном списке основных категорий информации, используемых для принятия решения «что производить?» — самая новая. Информация о покупателях становится жизненно важной в конкурентной борьбе. Например, определение типов посетителей супермаркетов становится основой для назначения новых режимов работы, размещения продуктов в залах, разработки системы скидок цены на продукты. Для успеха экономической деятельности предприятия стало критически важным привлечь и удержать потребителя. Для этой цели сбор информации о потребителях превращается в самостоятельную бизнес-задачу. Например, информация (знания) о покупателях конкретного района, хранящаяся в компьютерной базе данных, представляет серьезный коммерческий интерес для владельцев торговых точек этого района. Появляются специальные информационные системы для работы с покупателями — CRM (Customer Relationship Management).

Обратим внимание еще на несколько фактов, следующих из приведенного списка категорий информации. Собираемая информация призвана служить для решения задачи о будущем компании или организации, для которой она собирается. Она нужна, чтобы не упустить необходимости возможных изменений во всех сферах деятельности, чтобы сохранить предпринимательские позиции. Это стратегия получения или сохранения стратегического преимущества. Таким образом, информация на данном этапе превращается в стратегический ресурс.

Приведенный перечень разновидностей собираемой извне информации широк и объемен. Выходящая информация имеет более узкий набор адресов. Главный адрес выходящей информации компании — ее клиенты, потребители товаров и услуг. Информационная борьба за потребителей не утихает в мировой сети Интернет ни на минуту и представляет по сути главное содержание электронного бизнеса. Собственные сайты компаний обрушивают на потребителей потоки информации, сопровождаемые предложениями реальных возможностей приобрести продукт компании «здесь и сейчас». Специальные информационные системы CRM следят за отношениями между компанией и клиентом, стремятся

наладить доверительные и долгосрочные отношения, создать между ними постоянно действующий информационный мост.

Информационные процессы больше не могут быть отделены от бизнес-процессов компании. Информация более не является бюрократическим проклятием или необходимым злом — она органическая составляющая практически всех аспектов функционирования компании, ее основной и вспомогательной деятельности.

Таким образом, с позиций экономического анализа проявляется двойственный характер информации. С одной стороны — информация является товаром, обладающим специфическими свойствами, а с другой стороны — информация стратегический ресурс субъекта экономической деятельности. Но в обоих проявлениях фундаментальное свойство, связанное с обрабатываемой в процессе некой экономической деятельности информацией, — это ее безопасность.

Мера информации

Подводя итоги одного из межведомственных семинаров по проблемам информационной безопасности, ректор МГУ им. М. В. Ломоносова академик В. А. Садовничий посетовал, что, к сожалению, в большинстве случаев обсуждения носят сугубо гуманитарный характер: нет ни формального определения переменных, ни связывающих их соотношений.

Очевидным подходом к применению математических методов в сфере анализа безопасности информационных систем могло бы стать определение меры находящейся в системе информации. Используя аналогию с деньгами — как универсальной мерой количества и качества товаров и услуг — можно было бы пытаться строить количественную теорию информационной безопасности. Сомнительная перспектива такого подхода состоит в том, что можно определить несколько различных мер информации: синтаксическую, семантическую и прагматическую.

В качестве простейшей *синтаксической* меры информации может использоваться объем данных. Понятно, что эта мера никак не может характеризовать содержание данных, несущих некоторую информацию. В то же время во многих случаях уменьшение объема данных, хранимых на некотором носителе, может характеризовать нарушение информационной безопасности

(например, преднамеренное или случайное уничтожение таблиц базы данных).

Семантическая мера информации используется для измерения смыслового содержания информации. Необходимым элементом определения семантической меры информации является определение тезауруса. Тезаурус — это совокупность сведений и связей между ними, которыми располагает получатель информации. В некотором смысле тезаурус — это накопленные знания получателя.

Если приемником информации является персональный компьютер, тезаурус определяется совокупностью программ и аппаратных средств компьютера. Конкретный программно-аппаратный комплекс обеспечивает опосредованное использование тезауруса его создателей.

Если получателем является человек, его тезаурус — это арсенал его знаний. Поступившее сообщение обрабатывается с использованием имеющихся знаний с целью получения информации. Если тезаурус очень богат — арсенал знаний глубок и многообразен, он позволит извлекать информацию из практически любого сообщения. Маленький тезаурус, содержащий скудный багаж знаний, может стать препятствием для понимания сообщений, требующих лучшей подготовки.

Формально — количество семантической информации I_s, включаемой в дальнейшем в тезаурус, определяется соотношением тезауруса получателя S_i и содержанием передаваемой в сообщении информации S_0.

Рассмотрим случаи, когда количество семантической информации I_s равно или близко к нулю:

- при $S_i = 0$ получатель не воспринимает поступающую информацию;
- при $0 < S_i \leqslant S_0$ получатель воспринимает, но не понимает поступившую в сообщении информацию;
- при $S_i \to \infty$ получатель имеет исчерпывающие знания и поступающая информация не может пополнить его тезауруса.

При тезаурусе $S_i > S_0$ количество семантической информации I_s, получаемое из вложенной в сообщение информации S_0, вначале быстро растет с ростом собственного тезауруса получателя, а затем — начиная с некоторого значения S_i — падает.

Падение количества полезной для получателя информации происходит от того, что багаж знаний получателя стал достаточно солидным и пополнить его чем-то новым становится все труднее.

Прагматическая мера информации определяет полезность информации (ценность) для достижения получателем определенной цели. Эта мера также величина относительная, субъективная, обусловленная особенностями использования этой информации для принятия решения. В роли прагматической меры информации может служить приращение вероятности достижения цели.

Если до получения сообщения β вероятность достижения цели была p_0, а после получения сообщения стала p_1, то ценность информации, полученной из сообщения β можно оценить с помощью показателя I_p:

$$I_p = \log(p_1/p_0).$$

Если сообщение не изменило вероятность достижения цели и $p_1 = p_0$, ценность полученной с ним информации — нулевая.

Прагматическая мера информации может быть оценена величиной изменения целевой функции, обусловленным получением информации. В этом случае прагматическая мера измеряется в тех же самых единицах, в которых измеряется целевая функция. Целевая функция служит для определения экономического результата принятия решения (экономического эффекта) или проще — для количественной оценки конкретного варианта решения. Она может оценивать величину прибыли, получаемой в случае принятия данного решения или измерять величину соответствующих данному решению расходов имеющегося набора ресурсов (в килограммах, метрах, штуках и т. д.).

Желаемым результатом принятия решения должна быть либо наибольшая из всех возможных при данном наборе ресурсов прибыль, либо наименьшие расходы ресурсов, соответствующие выбранному решению. Тогда прагматическую меру (ценность) информации $I_\beta(\alpha)$, содержащейся в сообщении β, можно оценить по величине изменения целевой функции:

$$I_\beta(\alpha) = C(\alpha/\beta) - C(\alpha),$$

где $I_\beta(\alpha)$ — ценность сообщения β для системы α, $C(\alpha)$ — значение целевой функции, оценивающей экономический эффект функционирования системы α до получения сообщения β, $C(\alpha/\beta)$ — значение целевой функции, оценивающей эффект

функционирования системы α при условии, что будет использована информация, содержащаяся в сообщении β.

Реальные экономические системы в большинстве случаев имеют ясно формулируемые цели. Поэтому целесообразно при постановке задачи анализа информационной безопасности экономической системы опираться на прагматическую меру информации.

Структура свойства информационной безопасности экономической системы

В качестве задачи начального уровня (наиболее простой) поставим задачу сравнения двух проектных решений по обеспечению информационной безопасности двух вариантов систем. Для корректной постановки задачи необходимо прежде всего раскрыть существо понятия «информационная безопасность автоматизированной информационной системы».

Проблема обеспечения информационной безопасности экономической системы может быть определена как разработка методов и средств, обеспечивающих выполнение трех взаимосвязанных свойств системы [2]:

- конфиденциальности — обеспечения пользователям доступа только к данным, для которых пользователь имеет явное или неявное разрешение на доступ;
- целостности — обеспечения защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки;
- доступности — обеспечения возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией.

Методы и средства решения задач, обеспечивающих наличие в системе трех отмеченных взаимосвязанных свойств, характерны для любых информационных систем, используемых в управлении экономическими системами. В частности, для систем организационного управления и информационного обеспечения процесса принятия решений обеспечение конфиденциальности предусматривает комплекс мер по предотвращению доступа к конфиденциальной информации несанкционированными пользователями. К такой конфиденциальной информации предприятия, как

правило, относится технология производства конкретных товаров и услуг (know-how), сведения о клиентах, программы продвижения новых товаров и услуг.

Обеспечение целостности предусматривает комплекс мер по предотвращению несанкционированного изменения или уничтожения информации, используемой системой поддержки принятия решений конкретной фирмы или предприятия. Обеспечение целостности обычно критически важно для финансовых данных предприятия, данных о продажах и наличии товаров на складах.

Обеспечение доступности информации предусматривает систему мер по поддержке всем законным (например, зарегистрированным) пользователям доступа к ресурсам системы в соответствии с принятой технологией. В большинстве систем электронного бизнеса доступ пользователей к предоставляемым товарам и услугам обеспечивается круглосуточно.

Постановка задачи экономического анализа проектных решений

Перейдем к постановке задачи сравнения проектных решений по реализации механизмов обеспечения информационной безопасности экономической системы.

Существенной особенностью данной задачи является присутствие хорошо определенного антагонизма. Нарушитель, независимо от того, является он внешним или внутренним, стремится нанести ущерб защищающейся стороне. С позиций стороны защиты все нарушители, равно как и неблагоприятные стечения обстоятельств, деятельность конкурентов, могут рассматриваться как один противоборствующий защищающейся стороне объект.

В том случае, если нарушитель, независимо от его природы, получает некоторую выгоду, противоборствующая сторона терпит убыток. Следовательно в качестве класса моделей, из которого может быть осуществлен выбор конкретной модели, можно рассматривать теоретико-игровые модели антагонистических конфликтных ситуаций. Для того чтобы продолжить уточнение постановки задачи, необходимо определить и охарактеризовать множество возможных стратегий нападения и защиты и построить целевую функцию экономической системы. Для большинства информационных систем, используемых в экономике, естественно

предполагать, что существует конечное число уязвимостей системы. Это предположение лежит в основе большинства моделей безопасности. Для осуществления противодействия в отношении любой из уязвимостей проектировщик системы защиты также использует конечное число механизмов. Многие механизмы защиты повышают уровень защищенности системы по отношению к нескольким типам уязвимостей.

По своей сути задача обеспечения информационной безопасности любой экономической системы является недетерминированной, поскольку система находится в постоянном взаимодействии с внешней средой, включающей такие элементы, как случайную активность пользователей и случайное состояние среды (активность конкурентов, состояние природы, политическая и экономическая обстановка и т. п.). Для задач, характеризующихся значительной неопределенностью и высокой ответственностью за принимаемое решение, обычно применяется минимаксный критерий. Осуществляется поиск решения, которое в наихудшей для одного из антагонистов ситуации обеспечивает наилучшее с точки зрения его затрат (или прибыли) решение.

Проведенное рассуждение, построенное на анализе особенности содержательной постановки задачи, приводит к выводу о целесообразности использования матричной игры в качестве математической модели задачи сравнения проектных решений по обеспечению информационной безопасности экономических систем. Матричная игра задается матрицей выигрышей игроков [1]. Для определенности будем считать, что игрок A моделирует поведение стороны защиты, а игрок B моделирует поведение нарушителя (включая и пассивные неблагоприятные факторы). Пусть игрок A имеет m стратегий $A_1, \ldots, A_m$, а игрок B имеет n стратегий $B_1, \ldots, B_n$. Если игрок A выбрал стратегию A_i, а игрок B — стратегию B_j, то будем считать, что этот выбор стратегий однозначно определяет результат конкретной реализации игры — выигрыш a_{ij} игрока A и выигрыш b_{ij} игрока B, причем эти выигрыши связаны равенством $a_{ij} + b_{ij} = 0$. При анализе матричной игры можно рассматривать выигрыш только одного из игроков. Пусть это будет выигрыш игрока A. Матрицу выигрышей игрока A обозначим $A = (a_{ij})$, так, что $\dim(A) = m \times n$. Обычно эту матрицу называют матрицей игры. Критерий предпочтения игрока A состоит в том, что он выбирает максимально возможное

значение выигрыша при наихудшей ситуации. На содержательном уровне такой выбор критерия означает, что сторона защиты предполагает, что противник осуществляет наиболее эффективную стратегию нападения. Учитывая, что в качестве «противника» выступают и неуправляемые неблагоприятные факторы внешней среды, данный подход предполагает также, что строится наиболее эффективная защита для наихудшей в целом ситуации. Представляется, что для экономических систем, функционирующих в условиях острой конкурентной борьбы и недостаточной правовой защиты бизнеса такой подход оправдан.

Обозначим

$$\alpha = \max_i \alpha_i = \max_i \min_j a_{ij}, \quad \text{где } \alpha_i = \min_j a_{ij}. \tag{1}$$

Число α в этом случае называется нижней ценой игры.

Для игрока B предпочтительной будет стратегия, при которой обеспечивается минимально возможное значение проигрыша при наихудшей ситуации (то есть при максимально эффективной системе защиты).

Обозначим

$$\beta = \min_j \beta_j = \min_j \max_i a_{ij}, \quad \text{где } \beta_j = \max_i a_{ij}. \tag{2}$$

Число β называется верхней ценой игры.

В общем случае $\alpha \leqslant \beta$ [1]. Представляется, что это соотношение соответствует интуитивному представлению о том, что защищающаяся сторона находится в более сложных условиях, чем нападающая. Соответствие формального соотношения распространенному представлению о сущности моделируемого явления может служить дополнительным аргументом, обосновывающим выбор предложенной модели.

Если $\alpha = \beta = \nu$, то их общее значение называется ценой игры и обозначается ν. Цена игры ν совпадает со значением элемента $a_{i^* j^*}$ матрицы A, расположенного на пересечении i^*-той строки и j^*-столбца, определяющих значения α и β из соотношений (1) и (2) соответственно. Этот элемент называют седловой точкой матрицы A. Известно, что если игрок A выберет стратегию, отличающуюся от стратегии i^*, а игрок B будет придерживаться стратегии j^*, то выигрыш игрока A может только уменьшиться. Не всякая матрица, задающая игру, имеет

седловую точку. Поэтому рассматривается обобщение постановки задачи с введением рандомизации на множестве стратегий.

Случайная величина, значениями которой являются номера стратегий игрока, называются его смешанной стратегией. Задание смешанной стратегии игрока состоит в определении вероятностей, с которыми выбирается его стратегии. Для игрока A, имеющего m чистых стратегий, смешанная стратегия может быть описана набором m неотрицательных чисел $p_i \geqslant 0$:

$$P = \left\{ p_1, p_2, \ldots, p_m \;\middle|\; \sum_{i=1}^{m} p_i = 1,\ \ p_i \geqslant 0 \right\}.$$

Для игрока B, имеющего n чистых стратегий, соответствующее распределение вероятностей описывается набором n неотрицательных чисел:

$$Q = \left\{ q_1, q_2, \ldots, q_n \;\middle|\; \sum_{j=1}^{n} q_j = 1, q_j \geqslant 0 \right\}.$$

В качестве среднего выигрыша игрока A при использовании игроками смешанных стратегий (P, Q) естественно принять математическое ожидание выигрыша игрока A, которое равно:

$$H_{\mathrm{A}}(P, Q) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ik} p_i q_k.$$

Стратегии $P^* = \{p_1^*, p_2^*, \ldots, p_m^*\}$ и $Q^* = \{q_1^*, q_2^*, \ldots, q_n^*\}$ называются оптимальными смешанными стратегиями игроков A и B, если выполнены следующие соотношения:

$$H_{\mathrm{A}}(P, Q^*) \leqslant H_{\mathrm{A}}(P^*, Q^*) \leqslant H_{\mathrm{A}}(P^*, Q),$$

при этом

$$\nu = H_{\mathrm{A}}(P^*, Q^*) = \max_P \min_Q H_{\mathrm{A}}(P, Q) = \min_Q \max_P H_{\mathrm{A}}(P, Q).$$

Величина ν называется ценой игры. Известно, что любая матричная игра имеет решение, а, следовательно, и цену игры, в смешанных стратегиях [1]. По сути, цена игры — это среднестатистический выигрыш, который получает игрок A в том случае, если его противник реализует сильнейшую в рассмотренном смысле стратегию. В том случае, если игрок B отклонится от своей сильнейшей стратегии, выигрыш игрока A может только возрасти.

Обратим внимание на то, что для определения цены игры необходимо знание только матрицы A. Поскольку цена игры — это среднестатистический выигрыш, можно утверждать, что игра, моделирующая некоторую реальную ситуацию и имеющая большую цену, предпочтительнее для игрока A.

Проведенные рассуждения позволяют осуществить формальную постановку задачи сравнения различных проектных решений по обеспечению информационной безопасности экономических систем. Анализ уязвимостей системы позволяет сформулировать конечное число вариантов деструктивного воздействия на автоматизированную информационную систему конкретного предприятия. Имеющиеся в распоряжении проектировщика системы защиты ресурсы, средства и методы позволяют сформулировать конечное число механизмов противодействия деструктивному воздействию на систему. Реализация пары чистых стратегий приводит к потерям, выражаемым некоторым числом.

Получение оценки потерь, связанных с реализацией некоторой пары чистых стратегий, предлагается осуществить следующим образом. Пусть оценка ущерба при реализации j-й стратегии наступающей стороны есть b_j. Обобщенная стоимость реализации механизмов защиты, связанных с i-й стратегией стороны защиты, есть a_i. Предполагая или рассчитывая на основании некоторых оценок вероятность успешной реализации j-й стратегии наступающей стороны против i-й стратегией стороны защиты p_{ij}, получаем математическое ожидание потерь со стороны защиты:

$$a_{ij} = -b_j \cdot p_{ij} + (-a_i \cdot (1 - p_{ij})).$$

В предложенной модели выигрыш для любой чистой стратегии игрока A всегда неположительный, а в представляющих практический интерес случаях — отрицательный. Эта особенность модели отражает факт затратного характера всех механизмов защиты. Выгода от использования системы всегда связана с ее целевым назначением. Подсистема защиты требует дополнительной затраты ресурсов системы, давая лишь дополнительную уверенность в том, что система будет успешно функционировать и приносить прибыль, несмотря на неблагоприятную окружающую среду, в частности активные действия конкурентов.

Предельный (и недостижимый на практике) случай дается системой, функционирующей в лояльной внешней среде, на абсолютно надежных программно-аппаратных средствах и обслуживаемой персоналом, не допускающим ошибок. В этом случае цена соответствующей игры достигает нулевого значения, поскольку подсистема защиты не нужна и, следовательно, не требует никаких ресурсов. В остальных случаях осуществляется расчет цены соответствующей игры.

Из двух различных решений предпочтительным считается решение, дающее большую (ближайшую к 0) цену игры.

Для решения общей задачи сравнения проектных решений по обеспечению информационной безопасности экономических систем в предложенной постановке необходимо в каждом конкретном случае решить следующие частные задачи:

- определение перечня уязвимостей для информационной системы предприятия;
- определение перечня средств обеспечения конфиденциальности, целостности и готовности системы, реализуемых организационными и программно-аппаратными методами;
- разработка методики расчета элементов платежной матрицы.

Разработанная модель является статической и может применяться для принятия стратегических решений (долгосрочной перспективы). Более реалистическая модель должна использовать разработанные методики аудита состояния окружающей среды и соответствующие адаптации элементов матрицы выигрышей.

Выводы

В статье представлен подход к разработке проблемы экономики информационной безопасности. Предложенный подход основан на прагматической мере информации. В качестве первого шага представлена формальная постановка задачи сравнения проектных решений по обеспечению информационной безопасности экономических систем, которая базируется на теоретико-игровой модели противоборства. Развитие предложенного подхода может обеспечить экономическое планирование уровней информационной безопасности в организации, и к разработке вопросов экономики информационной безопасности, в частности, обоснования вложений в те или иные технологии.

Литература

[1] *фон Нейман Дж.*, *Моргенштерн О.* Теория игр и экономическое поведение. М.: Наука, 1970.

[2] *Пярин В. А.*, *Кузьмин А. С.*, *Смирнов С. Н.* Безопасность электронного бизнеса. М.: Гелиос АРВ, 2002.

[3] *Майминас Е. З.* Информационное общество и парадигма экономической теории. Выпуск экономики № 11, 1997. С. 86–95.

Приложение 1. Доктрина информационной безопасности Российской Федерации

Утверждена Поручением Президента Российской Федерации от 9 *сентября* 2000 *г.* № *Пр*-1895.

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

I. Информационная безопасность Российской Федерации

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей

собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие

задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации «О государственной тайне», Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения «информационного оружия» против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз

информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;
- развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения «информационного оружия»;
- разработка и создание механизмов формирования и реализации государственной информационной политики России;
- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

II. Методы обеспечения информационной безопасности Российской Федерации

5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;
- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также

инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:
- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:
- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы

информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

В сфере экономики. Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;
- кредитно-финансовая система;
- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные

угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;
- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

В сфере внутренней политики. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

- конституционные права и свободы человека и гражданина;
- конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;
- открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

- создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;
- активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики. К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;
- информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

- блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;
- распространение за рубежом дезинформации о внешней политике Российской Федерации;
- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;
- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;
- разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;
- совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
- совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- научно-технические кадры и система их подготовки;
- системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

- стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;
- создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);
- политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств — участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;
- активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

- сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;
- неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;
- серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;
- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники — это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

В сфере духовной жизни. Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

- достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;
- свобода массовой информации;
- неприкосновенность частной жизни, личная и семейная тайна;
- русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств-участников Содружества Независимых Государств;
- языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;
- объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

- деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;
- ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;
- возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;
- использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба

обороноспособности страны и безопасности государства, распространения дезинформации;

- неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

- развитие в России основ гражданского общества;
- создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;
- выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;
- совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;
- государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;
- формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;
- разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

- разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;
- введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;
- противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах. Основными объектами обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;
- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;
- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;
- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;
- обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны. К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;
- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются:

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;

- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;
- нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;
- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

В правоохранительной и судебной сферах. К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;
- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;
- деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;
- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;
- отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;

- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

- создание защищенной многоуровневой системы интегрированных банков данных оперативно-разыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;
- повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций. Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс; к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;
- совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;
- повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;
- прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;
- разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности — неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных

центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия». Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами — участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том

числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

III. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса,

основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;
- организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;
- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику России;
- организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации.

Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;
- создание организационно-правовых механизмов обеспечения информационной безопасности;
- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;
- разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;
- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;
- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;
- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;
- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;

- гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации

10. Основные функции системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы

местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации,

а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной

сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

* * *

Реализация первоочередных мероприятий по обеспечению информационной безопасности Российской Федерации, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом Российской Федерации.

Приложение 2. Приоритетные проблемы научных исследований в области информационной безопасности Российской Федерации

Одобрены секцией по информационной безопасности научного совета при Совете Безопасности Российской Федерации (протокол от 28 марта 2001 г. № 1).

Гуманитарные проблемы обеспечения информационной безопасности Российской Федерации

1. Исследование места и роли проблем информационной безопасности в становлении современного информационного общества.

2. Исследование проблем обеспечения баланса интересов личности, общества и государства в информационной сфере.

3. Исследование роли и места информационной безопасности в обеспечении военной, экономической, экологической, иных видов национальной безопасности.

4. Разработка единого понятийного аппарата (терминов и определений) в сфере информационной безопасности.

5. Научное обоснование основных направлений деятельности государственных ведомственных структур по обеспечению информационной безопасности Российской Федерации.

6. Национальные интересы России и информационное противостояние в современном мире.

7. Ценностная ориентация личности, ее информационное обоснование и информационная безопасность.

8. Информационная безопасность и политическая этика.

9. Информационное пространство и проблема целостности российского государства.

10. Изучение и прогнозирование социально-психологических последствий внедрения и широкого распространения современных информационных технологий.

11. Исследование исторических аспектов, современного состояния и возможности развития информационной деятельности зарубежных государств с использованием ими российских информационных систем для пропаганды своих интересов.

12. Разработка и научное обоснование системы мониторинга состояния информационной безопасности Российской Федерации.

13. Разработка информационно-динамической модели баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения.

14. Разработка правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере.

15. Проблемы правовой охраны, распределения прав собственности и прибыли (доходов) по результатам научно-технической деятельности, по вознаграждению авторов и лиц, содействующих использованию объектов интеллектуальной собственности.

16. Исследование места и роли СМИ в решении задач информационного обеспечения государственной политики Российской Федерации.

17. Развитие нормативной базы, направленное на сохранение и правовую защиту российской интеллектуальной собственности в информационной сфере.

18. Совершенствование правового обеспечения, регламентирующего создание и использование банков данных, а также иных информационных ресурсов, имеющих федеральное значение.

19. Разработка проблем правового регулирования в области технологической независимости.

20. Разработка механизма правового регулирования защиты и использования технологий двойного применения.

21. Разработка моделей и механизмов страхования информационных рисков.

22. Разработка правовых механизмов сотрудничества государств-участников СНГ в обеспечении коллективной информационной безопасности.

23. Разработка проблем правового регулирования в вопросах инвестиционной политики в области информационных технологий.

24. Разработка правовых механизмов регулирования в сфере производства и эксплуатации криптографических продуктов.

25. Разработка правовых механизмов регулирования электронного документооборота.

26. Проблемы правового обеспечения создания и функционирования системы мониторинга угроз информационных атак на критически важные сегменты информационной инфраструктуры Российской Федерации.

27. Совершенствование нормативно-методической базы проведения экспертизы и контроля качества защиты информации и информационных ресурсов.

28. Разработка международно-правовых механизмов сдерживания информационного противоборства.

29. Гармонизация отечественных и зарубежных стандартов в области информационных технологий.

30. Проблемы формирования международной системы информационной безопасности.

31. Разработка моделей и правовых механизмов взаимодействия Центра и субъектов Российской Федерации в информационной сфере.

32. Разработка моделей и правовых механизмов взаимодействия органов власти субъектов Российской Федерации и органов местного самоуправления в информационной сфере.

33. Разработка и научное обоснование путей обеспечения информационно-психологической безопасности личности и общества.

Научно-технические проблемы обеспечения информационной безопасности Российской Федерации (физико-математические, технические)

34. Разработка концептуальной взаимоувязанной структуры информационного пространства и состава информационных ресурсов.

35. Проблемы создания и развития информационной составляющей информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти (ИТКС).

36. Исследование проблем обеспечения информационной безопасности национальных платежных систем на базе российских интеллектуальных карт.

37. Исследование проблем создания и развития национальной системы управления цифровыми сертификатами.

38. Поиск путей решения проблемы создания единой системы технических стандартов информационного обмена (протоколов, форматов данных, спецификаций интерфейсов) с учетом существующих международных стандартов и перспектив их развития.

39. Исследование подходов к созданию отечественной системы промышленных стандартов проектирования и разработки информационных систем и систем телекоммуникаций с учетом существующих международных стандартов и перспектив их развития.

40. Исследования, направленные на создание комплекса отечественных инструментальных средств проектирования информационных систем.

41. Проблемы совершенствования отечественного программного обеспечения.

42. Разработка и обоснование систем сертификации средств, содержащих элементы импортного производства.

43. Анализ возможности использования технологических особенностей производства новейших зарубежных и отечественных образцов элементной базы микроэлектроники для реализации деструктивных информационных функций.

44. Исследование проблем создания и функционирования национального эталонного банка доверенного программного обеспечения.

45. Исследование проблем создания и развития защищенных информационно-телекоммуникационных систем, в том числе разработка методов выбора архитектуры и расчета параметров этих систем, математических моделей и технологий управления, системного и прикладного программного обеспечения с интеграцией функций защиты, средств взаимодействия, устройств передачи и распределения информации.

46. Разработка моделей угроз безопасности систем и способов их реализации, определение критериев уязвимости и устойчивости систем к деструктивным воздействиям, разработка методов и средств мониторинга для выявления фактов применения несанкционированных информационных воздействий, разработка методологии и методического аппарата оценки ущерба от воздействия угроз информационной безопасности.

47. Разработка методов и средств проведения экспертизы и контроля качества защиты информации и информационных ресурсов, в том числе вопросов оценки базовых общесистемных программных средств на соответствие требованиям информационной безопасности.

48. Разработка методов и средств обеспечения информационной безопасности информационных и телекоммуникационных систем, в том числе автоматизированных систем управления безопасностью, методов и средств распределения ключей и защиты информации и информационных ресурсов от несанкционированного доступа и разрушающего информационного воздействия, антивирусных технологий, методов и средств контроля состояния защищенности от НСД современных и перспективных технических средств и каналов связи, решение проблемы гарантированного уничтожения остаточной информации на магнитных носителях, исследование и развитие методов построения защищенных систем, использующих ненадежные (с точки зрения информационной безопасности) элементы, включая проблему их тестирования.

49. Исследование проблем безопасности общероссийской информационной инфраструктуры в условиях ее вхождения в глобальные инфраструктуры.

50. Исследование проблем обеспечения информационной безопасности ИТКС, в том числе разработка нормативно-технической документации по безопасности, автоматизированных систем управления безопасностью, унифицированного ряда средств криптографической защиты с учетом используемых в ИТКС технологий обработки информации.

51. Исследование проблем информационной безопасности корпоративных сетей, в том числе сетей науки и образования (в рамках комплексной программы Минпромнауки России «Научное, научно-методическое, материально-техническое и информационное обеспечение системы образования»).

52. Проблемы лицензирования деятельности в области информационно-телекоммуникационных систем.

53. Анализ тенденций в развитии глобальной информационной сети и состояния участия в ней России.

54. Разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики.

55. Разработка криптографических проблем создания перспективных отечественных шифрсистем (в частности, высокоскоростных).

56. Разработка и обоснование новых методов криптографического анализа современных шифрсистем.

57. Разработка перспективных криптографических протоколов взаимодействия абонентов в сложных иерархических глобальных сетях и распределенных информационно-аналитических системах.

58. Исследование существующих и разработка новых систем с открытым ключом, соответствующих этим системам схем аутентификации и электронной цифровой подписи.

59. Совершенствование нормативно-методической базы по вопросам защиты информации с применением криптографических средств.

60. Анализ основных направлений и тенденций развития отечественных и зарубежных средств криптографической защиты информации.

61. Анализ возможности использования достижений физики и техники для получения доступа к информации, обрабатываемой

на современных технических средствах, в том числе исследование физических основ утечки информации от технических средств по побочным каналам, разработка проблем аналитической обработки побочных сигналов.

62. Исследование алгоритмических и технологических особенностей новейших зарубежных и отечественных технических средств обработки информации.

63. Исследование проблем и методов информационного доступа к каналам связи.

64. Разработка методологии оценивания защищенности, комплексных методов и средств защиты технических средств обработки информации от физико-технических методов несанкционированного доступа, совершенствование соответствующей нормативной базы.

65. Разработка проблем создания технических средств обработки информации, защищенных от физико-технических методов информационного доступа.

66. Сравнительный анализ тенденций развития физико-технических проблем защиты информации в стране и за рубежом.

67. Исследование архитектурных вариантов построения вычислительных систем высокой производительности, алгоритмического и программного обеспечения с учетом особенностей криптографических задач.

68. Исследование проблем построения автоматизированных систем обработки криптографической информации в неоднородной вычислительной среде.

69. Исследование проблем управления распределенными вычислительными процессами.

70. Разработка и научное обоснование моделей угроз и стратегий защиты объектов от технических разведок.

71. Разработка методов и средств противодействия техническим разведкам с учетом эффективности их функционирования.

72. Разработка методов и средств контроля состояния и достаточности принимаемых мер по противодействию техническим разведкам на объектах защиты.

73. Разработка современной методологии обеспечения противодействия техническим разведкам на объектах защиты.

74. Разработка, теоретическое и экспериментальное исследование современных методов стеганографии, других средств тайнописи и защиты от подделки.

75. Исследование и разработка отечественных защитных экранов с учетом моделей угроз для уже существующих и перспективных цифровых АТС.

Проблемы кадрового обеспечения информационной безопасности Российской Федерации

76. Обоснование облика, структуры и путей реализации единой системы подготовки кадров в области современных информационных технологий и информационной безопасности.

77. Обоснование структуры и функций Учебно-методического комплекса по подготовке, повышению квалификации и переподготовке кадров в области информационной безопасности.

78. Разработка государственных образовательных стандартов по новым специальностям высшего профессионального образования.

79. Создание нормативно-правовой базы особого порядка лицензирования образовательной деятельности в области информационной безопасности.

80. Проблемы нормативно-правового обеспечения подготовки специалистов по вопросам информационной безопасности и смежных областях.

81. Развитие нормативной базы, направленной на сохранение интеллектуального потенциала государственных вузов Российской Федерации, осуществляющих подготовку специалистов в области современных информационных технологий и информационной безопасности.

82. Разработка методик, специальной и учебной литературы по специальностям в области информационной безопасности, включая разработку учебных пособий для подготовки специалистов в области криптографии.

83. Разработка методик, специальной и учебной литературы по изучению общих вопросов информационной безопасности

в специальностях, не отнесенных к группе «Информационная безопасность».

84. Разработка базового мультимедийного учебно-методического комплекса по подготовке специалистов в области информационной безопасности и информационного противоборства.

85. Разработка методик, специальной и учебной литературы для курсов переподготовки и повышения квалификации кадров в области информационной безопасности.

86. Программные и аппаратные средства реализации современных информационных технологий в образовательном процессе.

87. Проблема использования в образовательном процессе деловых и специальных исследовательских игр по информационной безопасности.

НАУЧНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под ред. В. П. Шерстюка

Издательство Московского центра непрерывного математического образования. 119002, Москва, Большой Власьевский пер., 11.

Лицензия ИД № 01335 от 24.03.2000 г. Подписано к печати 25.02.2004 г. Формат 60 × 90/16. Печать офсетная. Объем 13 п. л. Тираж 500 экз. Заказ № .

Отпечатано с готовых диапозитивов в ППП «Типография „Наука“». 119099, Москва, Шубинский пер., 6.