Предисловие

Завершается десятилетний период практической реализации положений Доктрины информационной безопасности Российской Федерации, утвержденной Президентом РФ 09 сентября 2000 г. Отражая основы государственной политики в отношении целей, задач, принципов и основных направлений обеспечения информационной безопасности Российской Федерации, Доктрина заложила фундамент для дальнейшего совершенствования правового, методического, научно-технического, технологического и организационного аспектов информационной безопасности России.

Подводя итоги этого периода, можно сделать вывод: несмотря на все сложности социально-экономического развития России за прошедшие годы в сфере обеспечения информационной безопасности, сделан заметный шаг вперед и по ряду направлений достигнут паритет со многими информационно развитыми зарубежными странами.

Так, по направлению научно-технического и технологического обеспечения создана современная развитая индустрия средств, комплексов, работ и услуг по защите информации ограниченного доступа, имеющая явно выраженный рыночный характер. Темпы развития этого сегмента рынка в целом значительно превосходили даже темпы роста всего рынка ИТ-технологий.

Получило дальнейшее развитие и направление организационно-правового обеспечения. Хотя его достижения и уступают научно-техническим и технологическим результатам и многие вопросы правового регулирования остаются нерешенными, но уже можно констатировать наличие солидной законодательной базы и хороших предпосылок для ее совершенствования. По данному направлению успешно защищено две диссертации на соискание ученой степени доктора юридических наук и более десяти кандидатских работ по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Особо необходимо отметить, что принятие Доктрины информационной безопасности РФ дало мощный толчок к развитию такой важной составляющей обеспечения информационной безопасности, как подготовка кадров. Уже более десяти лет достаточно эффективно функционирует государственная система подготовки молодых специалистов по семи специальностям направления «Информационная безопасность», объединяющая около ста вузов. На рыночной

основе достаточно бурно развивается сфера услуг дополнительного профессионального образования.

Все это дало возможность постановки задачи массового обучения (всеобуча) всех ИТ-специалистов и пользователей компьютерных систем вопросам обеспечения информационной безопасности наряду с решением задачи повышения компьютерной грамотности всего населения страны. Вместе с тем, решение данной задачи сдерживается недостаточной обеспеченностью необходимыми учебно-методическими материалами.

Настоящее учебное пособие, по мнению авторов, является важным шагом в этом направлении и позволяет в дальнейшем продолжить накопление соответствующего учебно-методического потенциала всеобуча в области информационной безопасности.

В пособии в систематизированном виде изложены основы современных знаний в области информационной безопасности, апробированные в практической деятельности государственной системы защиты информации за последние десятилетия.

Во введении, первой и второй главе изложены концептуальные и методологические аспекты информационной безопасности, ретроспектива и направления развития этой сферы научно-технической деятельности на ближайшую перспективу.

В третьей, четвертой, пятой и шестой главах рассмотрены методы решения основных задач информационной безопасности в области защиты информации от несанкционированного доступа, криптографические методы защиты информации, методы противодействия утечке информации по техническим каналам и вредоносному программному обеспечению (компьютерным вирусам).

В седьмой главе анализируется современное состояние организационно-правового обеспечения информационной безопасности как на государственном, так и на объектовом уровне защиты информации.

Восьмая глава посвящена анализу проектирования комплексных систем защиты информации при автоматизированной обработке данных.

Учебное пособие подготовлено коллективом преподавателей факультета «Информационная безопасность» НИЯУ МИФИ. Введение, гл. 1, 2 написаны к.т.н., профессором А.А. Малюком, гл. 3, 6, 8 — д.т.н., профессором В.И. Королевым , гл. 4 — д.ф.-м.н., доцентом В.М. Фомичевым, гл. 5 — к.т.н. А.П. Дураковским, гл. 7 — доцентом Т.А. Кондратьевой (в части правового обеспечения) совместно с к.т.н., доцентом В.С. Горбатовым. Общая редакция учебного пособия и организационная поддержка при подготовке к изданию осуществлены доцентом В.С. Горбатовым.

Введение

Качественные изменения в экономической, социально-политической и духовной сферах общественной жизни, обусловленные интенсивным развитием и использованием современных информационных технологий, обозначили движение человечества к новой, постиндустриальной фазе развития — информационному обществу.

Отличительные черты информационного общества:

- существенное увеличение доли в валовом внутреннем продукте отраслей экономики, связанных с производством знаний, с созданием и внедрением наукоемких, в том числе информационных, технологий, других продуктов интеллектуальной деятельности, с оказанием услуг в области информатизации, образования, связи, а также поиска, передачи, получения и распространения информации (информационных услуг);
- радикальное ускорение технического прогресса, превращение научных знаний в реальный фактор производства, повышение качества жизни человека и общества;
- участие значительной части трудоспособного населения в производственной деятельности, связанной с созданием и использованием информационных технологий, информации и знаний;
- глобализация экономической, политической и духовной сфер жизни общества.

В связи с этим проблемы совершенствования информационных систем во всех сферах общественной деятельности считаются в настоящее время одними из наиболее актуальных и неотложных задач современного общества. С целью их решения в последние годы ведутся весьма интенсивные и крупномасштабные исследования и разработки.

Вместе с тем, расширение созидательных возможностей на основе интенсивного развития информационного общества создает предпосылки для появления новых угроз национальной безопасности. Они связаны с нарушением установленных режимов использования информационных и коммуникационных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также использованием возможностей современных информационных технологий для осуществления враждебных, в том числе террористических и других преступных действий.

Таким образом, проблема обеспечения информационной безопасности и, прежде всего, надежной защиты информации от ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования приобретает в этих условиях особую остроту.

Вообще говоря, проблема защиты информации имеет многовековую историю. Однако, концентрируя внимание на актуальных задачах сегодняшнего дня, ограничимся лишь тем периодом, который характеризуется регулярным применением для сбора, хранения, обработки и передачи информации средств вычислительной техники и создания на их основе автоматизированных систем (АС). Проблемы защиты информации в таких системах возникли практически одновременно с появлением самих систем. Однако особо они обострились, когда АС стали применяться для обработки секретной информации. Условия общей закрытости и изолированности в советский период развития нашей страны привели к такому положению, когда чуть ли не все содержание проблемы свелось к защите только секретной информации. Сегодня стало ясно, что этот аспект, несмотря на всю свою значимость, составляет лишь одну из частей гораздо более общей задачи обеспечения защиты жизненно важных интересов личности, общества и государства в информационной сфере.

В более широкой постановке проблемы защиты информации в СССР стали открыто обсуждаться (сначала достаточно робко) немногим более тридцати лет назад после того, как в 1975–1976 гг. в журнале «Зарубежная радиоэлектроника» был опубликован цикл из шести обзорных статей, подготовленных по данным зарубежной печати. Интенсивность обсуждения проблемы, исследований и разработок в этой области непрерывно росла, и к настоящему времени практически сформировалось самостоятельное научно-техническое направление. Создана также система подготовки профессиональных специалистов по защите информации. Иными словами, мы сегодня фактически имеем дело с новой важной сферой деятельности, в которой занято достаточно представительное число специалистов.

Основные направления данной деятельности:

- организация практических работ по защите информации, управление ими и их правовое обеспечение на государственном, ведомственном, региональном и объектовом уровнях;
- проведение научных исследований всех аспектов рассматриваемой проблемы, разработка, производство и распространение средств защиты;
- подготовка кадров по защите информации.

Рассматривая общее содержание указанных направлений, мы можем отметить, что по первому из них, в плане правового обеспечения и организации работ по защите информации, к настоящему времени на государственном уровне создана достаточно стройная и эффективная система управляющих органов. Основу этой системы составляют такие государственные структуры, как Совет Безопасности, Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности, Министерство внутренних дел РФ и др.

Что касается объектового уровня, то в настоящее время практически на всех объектах (предприятиях, учреждениях, других организациях), деятельность которых связана с обработкой подлежащей защите информации, создаются штатные службы защиты, состав и численность которых определяются объемом соответствующих задач. По общему признанию существующие службы решают свои задачи более или менее эффективно. Однако те изменения, которые происходят в понимании существа проблемы защиты информации, подходах, методах и средствах ее решения, предопределяют необходимость существенной корректировки организации и содержания их работы. В частности, расширение рамок комплексности защиты требует наличия в составе соответствующих служб высококвалифицированных специалистов по различным видам защиты информации. Непрерывный рост арсенала средств защиты, способов и методов их применения требует для получения наибольшего эффекта оптимального комплексирования всех средств и методов, т.е. создания комплексных (как по целям, так и по средствам) систем защиты и организации соответствующего управления ими. При этом особенностью этих систем является то, что они должны эффективно функционировать в условиях неопределенности, а зачастую и непрогнозируемости проявления дестабилизирующих факторов.

Кроме того, непрерывный рост количества объектов, нуждающихся в защите информации, но не имеющих возможностей содержать собственную полноценную службу защиты, делает все более актуальной задачу развития аутсорсинга в сфере обеспечения информационной безопасности и создания для этих целей специализированных центров защиты информации. Создание сети таких центров представляется главным методом организационного решения проблемы защиты информации на региональном и ведомственном уровне.

Анализируя результаты научных исследований и разработок в области защиты информации, производства и распространения средств защиты, следует отметить, что на предшествующем этапе усилия были направлены на создание новых средств (технических,

программно-аппаратных, криптографических) и способов построения на их основе комплексных механизмов и систем защиты. Современный период развития информатизации общества характеризуется рядом новых обстоятельств, заставляющих внести существенные коррективы в изначальную постановку задачи защиты информации.

Во-первых, поскольку все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, формируется задача обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации.

Во-вторых, с самого начала регулярного использования автоматизированных технологий обработки информации актуальной стала задача обеспечения требуемого качества информации. Причем с течением времени актуальность данной задачи возрастает, а сама задача усложняется. В содержании задач обеспечения необходимого уровня качества информации и информационной безопасности много общего и аналогичного, что естественным образом приводит к единству концептуальных и методологических основ их решения.

В-третьих, одним из серьезных достижений современной информатики следует признать разработку концепции информационного кадастра, осуществленную в 90-х годах прошлого века профессором В.А. Герасименко. Информационный кадастр представляет собой высокоорганизованную совокупность данных, необходимых для эффективной деятельности соответствующего объекта (предприятия, учреждения, иной организации). Концепция информационного кадастра является ядром более общей концепции информационного обеспечения деятельности объектов. При этом, естественно, должны быть учтены и все задачи защиты информации, защиты от информации и обеспечения качества информации, которые необходимо решать как при формировании информационного кадастра, так и при его поддержке и использовании. Возникает обобщенное понятие управления информацией, объединяющее все упоминавшиеся выше понятия.

В-четвертых, серьезное внимание на новом этапе развития должно быть уделено совершенствованию методов и инструментальных средств, обеспечивающих решение любых возникающих задач защиты информации на регулярной основе.

Таким образом, можно говорить о наличии объективной необходимости создания методологических основ решения задач защиты информации, обеспечивающих переход от экстенсивных к интенсивным способам защиты.

Основное концептуальное требование к средствам защиты в условиях такого перехода может быть сформулировано в терминах достаточности в том смысле, что в их арсенале должны быть средства для решения любой задачи и в любых потенциально возможных условиях.

Резюмируя вышесказанное, можно констатировать, что на сегодня наиболее острой является проблема комплексного подхода к развитию теории и практики защиты информации. Объективная необходимость постановки проблемы комплексной защиты информации обусловлена системным характером влияния на ее безопасность большой совокупности различных обстоятельств, имеющих к тому же различную физическую природу и различные целевые посылки. Очевидно, что в этих условиях адекватным современным потребностям и условиям защиты информации может быть только комплексный подход к решению данных проблем.

Под комплексной защитой информации будем понимать целенаправленное применение в системах ее обработки различных средств, методов и мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения ее безопасности. При этом само понятие комплексности является сложным и включает в себя, по крайней мере, следующие аспекты:

- защита по всей совокупности показателей защищенности информации и всей совокупности факторов, на нее влияющих (целевая комплексность);
- непрерывная защита информации в течение всего времени и на всех этапах жизненного цикла АС (временна́я комплексность);
- реализация проблем защиты в общей совокупности всех проблем развития, построения и использования АС (концептуальная комплексность).

Временна́я комплексность, как это сформулировано выше, предполагает непрерывность осуществления мероприятий по защите информации и притом не только в процессе ее непосредственной автоматизированной обработки, но и на всех других этапах жизненного цикла АС. Заметим, что это обстоятельство предполагает организацию и обеспечение целенаправленного управления всей совокупностью этих мероприятий.

Концептуальная комплексность интерпретируется в том смысле, что потребности, возможности и условия защиты информации должны органически учитываться в концепциях построения и организации функционирования АС, а в более широком смысле — в целом при решении проблем информатизации общества.

Из изложенного материала следует, что на систему комплексной защиты информации возлагается:

- обеспечение физической целостности, т.е. заданной синтаксической структуры защищаемой информации;
- обеспечение логической целостности, т.е. семантических характеристик информации и установленных взаимосвязей между ее элементами;
- обеспечение доверия к информации в прагматическом плане, т.е. предупреждение ее несанкционированной модификации даже при сохранении синтаксических и семантических характеристик;
- предупреждение несанкционированного получения защищаемой информации лицами, не имеющими на это специальных полномочий, т.е. обеспечение установленного статуса ее конфиденциальности;
- предупреждение копирования информации без санкции ее обладателя.

Комплексная защита должна предусматривать нейтрализацию негативного воздействия на информацию всех потенциально возможных дестабилизирующих факторов, а именно:

- стихийных бедствий, которые могут происходить в пределах системы обработки или в окружающей среде;
- злоумышленных и незлоумышленных действий людей, причем как посторонних лиц, так и лиц, входящих в состав системы обработки;
- побочных влияний, которые может оказывать окружающая среда.

Естественно, что все задачи, возлагаемые на систему комплексной защиты информации, должны реализовываться при неукоснительном соблюдении требования по обеспечению необходимого уровня ее доступности. Иначе самой защищенной будет та АС, к которой никто не имеет физического доступа.

Что касается третьего направления, проблемы кадрового обеспечения информационной безопасности, то следует отметить, что данный вопрос к настоящему времени применительно к защите информации имеет достаточно серьезную практическую реализацию и некоторые теоретико-методологические обобщения. Справедливость сказанного можно подтвердить тем, что на сегодняшний день в стране уже функционирует организованная система подготовки молодых, переподготовки и повышения квалификации работающих специалистов по защите информации. Ее основу составляют учебно-методическое объединение вузов по образованию в области информацион-

ной безопасности и сеть региональных учебно-научных центров высшей школы. Подготовку кадров в соответствии с Государственными образовательными стандартами семи специальностей направления «Информационная безопасность» осуществляют более 100 вузов страны. Соответствующий образовательный стандарт введен и для учреждений среднего профессионального образования. На очереди решение задачи организации своеобразного «всеобуча», основу учебно-методического обеспечения которого может составить настоящее учебное пособие.