А. А. Малюк

ЗАЩИТА ИНФОРМАЦИИ: СОВРЕМЕННЫЕ ПРОБЛЕМЫ

Интенсивное развитие и использование современных информационных технологий привели в настоящее время к серьезным качественным изменениям в экономической, социально-политической и духовной сферах общественной жизни. Человечество фактически переживает этап формирования нового информационного общества.

Принятая в 2008 г. Стратегия развития информационного общества в России так характеризует его отличительные черты:

- существенный рост 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 в области поиска, передачи, получения и распространения информации;
- радикальное ускорение технического прогресса, превращение научных знаний в реальный фактор производства, повышения 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 этих условиях на передний план экономического и социального развития выходят проблемы совершенствования систем информационного обеспечения всех сфер деятельности общества. Их решению в последние годы посвящаются интенсивные и крупномасштабные исследования и разработки [1].

Вместе с тем развитие информационного общества, помимо расширения созидательных возможностей, приводит и к росту угроз национальной безопасности, связанных с нарушением установленных режимов использования информационных и коммуникационных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также с использованием возможностей современных информационных технологий для осуществления враждебных, террористических и других преступных действий [2]. В связи с этим особую остроту сегодня приобретает проблема обеспечения информационной безопасности, и прежде всего надежной защиты информации (предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования).

Вообще говоря, проблема защиты информации, имея многовековую историю, приобрела особую актуальность только во второй половине XX в., которая характеризуется постоянно

растущей интенсивностью развития средств вычислительной техники. Проблемы защиты информации особо обострились, когда эти средства стали применяться для обработки закрытой информации. Причем нередко проблему защиты информации стали сводить к защите только секретной информации, хотя, как сегодня стало ясно всем, это составляет лишь одну из частей гораздо более общей задачи обеспечения защиты жизненно важных интересов личности, общества и государства в информационной сфере.

Сегодня мы можем констатировать, что в процессе своего развития мировая цивилизация пришла к формированию самостоятельного научно-технического направления «Информационная безопасность» и созданию системы подготовки профессиональных специалистов по защите информации. Иными словами, в настоящее время мы фактически имеем дело с новой важной сферой деятельности, в которой занято достаточно представительное число людей [3]. Основными задачами данной сферы являются:

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

Рассматривая общее содержание перечисленных задач, мы можем отметить, что в плане организации работ по защите информации в Российской Федерации 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 безопасности, Федеральная служба по техническому и экспортному контролю, Министерство внутренних дел Российской Федерации и др.

На уровне объектов информатизации (предприятия, учреждения, другие организации) работа по защите информации организуется штатными службами защиты, состав и численность которых определяются объемом соответствующих задач. Как показывает анализ деятельности данных служб, на сегодня они решают свои задачи более или менее эффективно. Однако изменения в понимании существа проблемы защиты информации, в подходах, методах и средствах ее решения, которые связаны с активным формированием информационного общества, предопределяют необходимость существенной корректировки организации и содержания их работы. В частности, расширение рамок комплексности защиты требует наличия в составе соответствующих служб высококвалифицированных специалистов по техническим, организационным, правовым и гуманитарным аспектам защиты информации, а непрерывный рост арсенала предлагаемых на рынке средств защиты, способов и методов их применения требует оптимального их комплексирования (как по целям, так и по видам), а также организации оптимального управления ими. При этом отличительной особенностью проблемы защиты информации является то, что ее решение должно осуществляться в условиях неопределенности, а зачастую и непрогнозируемости проявления дестабилизирующих факторов.

Кроме того, непрерывный рост количества объектов информатизации, 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 уровне.

Анализируя доступные результаты научных исследований и разработок в области защиты информации, можно с достаточной степенью уверенности утверждать, что до последнего времени данные разработки в основном были направлены на развитие технических средств защиты

(физических, программно-аппаратных, криптографических). Современный же период развития информатизации общества, как это уже отмечалось, характеризуется рядом новых обстоятельств, заставляющих внести существенные коррективы в изначальную постановку задачи защиты информации.

Во-первых, поскольку с развитием информационного общества все большую актуальность приобретает задача защиты людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, то можно говорить о полномасштабной постановке проблемы обеспечения информационной безопасности как органической совокупности процессов защиты информации и защиты от информации. Впервые именно такая постановка проблемы обеспечения информационной безопасности была рассмотрена в работе [4].

Во-вторых, постоянно возрастающая зависимость всех сфер жизнедеятельности информационного общества от реализации автоматизированных технологий обработки информации сделала особо актуальной задачу обеспечения требуемого качества информации. В содержании задач обеспечения необходимого уровня качества информации и информационной безопасности много общего, что естественным образом приводит к единству концептуальных и методологических основ их решения.

В-третьих, одним из серьезных достижений современной информатики следует признать разработку профессором В. А. Герасименко концепции информационного кадастра как организованной совокупности данных, необходимых для эффективной деятельности соответствующего объекта информатизации [5]. Концепция информационного кадастра является ядром информационного обеспечения деятельности объектов. При этом при его формировании, естественно, должны быть учтены и все потребности решения задач защиты информации, защиты от информации и обеспечения качества информации. Таким образом, возникает обобщенное понятие управления информацией, объединяющее все упоминавшиеся выше понятия.

В-четвертых, серьезное внимание на современном этапе должно быть уделено совершенствованию методов и инструментальных средств, обеспечивающих решение любых возникающих задач, как защиты информации, так и защиты от информации.

Иными словами, сегодня можно говорить о вызревании объективной необходимости создания методологических основ решения задач обеспечения информационной безопасности, и прежде всего защиты информации, т. е. о переходе от экстенсивных к интенсивным способам защиты, характеризующимся широкомасштабным использованием всех научно-технических и инновационных достижений в этой области. Это естественным образом влечет за собой приоритетное формирование теории защиты информации.

Фундамент основ теории защиты информации был заложен на предшествующем этапе рядом работ российских ученых, в том числе выполнявшихся под руководством профессора В. А. Герасименко в стенах Московского инженерно-физического института. В результате этих исследований было введено понятие стратегии защиты и обосновано базовое множество необходимых стратегий, предложена унифицированная концепция защиты информации (УКЗИ), обосновано полное множество задач, подлежащих решению в процессе защиты информации [6].

Углубленное изучение проблемы формирования научно-методологического базиса теории защиты информации как краеугольного камня интенсификации процессов обеспечения информационной безопасности привело нас к выводу, что эффективное решение задач защиты возможно только с учетом органической связи всего комплекса проблем развития информационного общества (научно-технических, организационно-правовых, гуманитарных). При этом в силу отмеченной специфики методологической основой теории должны являться неформально-эвристические подходы, учитывающие все многообразие дестабилизирующих факторов, в том числе связанных с особенностями поведения человека — члена информационного общества.

Остановимся еще на двух задачах деятельности в области защиты информации. Первая — это исследование, разработка и распространение средств защиты, которым всегда уделялось и продолжает уделяться большое внимание. Отметим здесь, что основным концептуальным требованием к средствам защиты в условиях перехода к интенсивным способам защиты должна быть их достаточность (в их арсенале должны быть средства для решения любой задачи и в любых потенциально возможных условиях).

Другая задача — это кадровое обеспечение информационной безопасности. Следует отметить, что данный вопрос к настоящему времени применительно к защите информации имеет в стране достаточно серьезную практическую реализацию и некоторые теоретико-методологические обобщения. На сегодняшний день уже более десятилетия функционирует организованная система подготовки молодых и повышения квалификации работающих специалистов по защите информации, основой которой являются учебно-методическое объединение вузов по образованию в области информационной безопасности и сеть региональных учебно-научных центров высшей школы. Следующая задача в этой области заключается в создании четкой государственной системы прогнозирования потребности в специалистах, в разработке методологии формирования государственного заказа на подготовку, в развитии новых направлений и образовательных программ подготовки кадров, учитывающих принципиально междисциплинарный характер данной области деятельности.

Резюмируя, можно выделить следующие, на наш взгляд, наиболее острые на сегодня проблемы развития теории и практики защиты информации:

1) создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы защиты информации в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);

2) разработка научно обоснованных подходов к формированию нормативно-методических документов по защите информации;

3) разработка методологии стандартизации подходов к созданию систем защиты информации и рационализации схем и структур управления защитой на объектовом, региональном и государственном уровнях.

Решение всего спектра перечисленных задач имеет важное значение для реализации положений Концепции национальной безопасности Российской Федерации, Доктрины информационной безопасности и Стратегии развития информационного общества в России.

Таким образом, представляется, что основная цель и направленность научных исследований в области обеспечения информационной безопасности заключается сегодня в разработке концептуальных и методологических основ интенсификации процессов защиты информации и рационализации подходов к организации систем защиты и управлению их функционированием.

В соответствии с этим можно было бы следующим образом сформулировать программу исследований:

· определение места проблем защиты информации в общей совокупности информационных проблем современного общества;

· исследование подходов к защите информации и обоснование необходимости перехода в современных условиях к интенсивным способам защиты;

· разработка концептуально-методологических основ интенсификации процессов защиты информации;

· создание методологии оценки уязвимости информации;

· разработка методов определения требований к защите информации с учетом факторов, влияющих на уровень защиты, и потенциально возможных условий функционирования защищаемых систем;