ВВЕДЕНИЕ

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. Феномен резко возрастающего влияния информационно-коммуникационных технологий на формирование общества XXI века был отмечен в Окинавской Хартии глобального информационного общества, принятой лидерами «восьмерки» 22 июля 2000 г.

Утвержденная в 2008 году 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 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 коммуникацион-

ных 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 самостоятельную актуальность только во второй половине XX века, которая характеризуется бурным развитием средств вычислительной техники. Причем особая острота проблемы была связана с тем, что указанные средства стали применяться и для обработки закрытой информации. В связи с этим и по сей день нередко проблему защиты информации сводят к защите только секретной информации, хотя, как сегодня стало ясно всем, это составляет лишь одну из частей гораздо более общей задачи обеспечения целостности, доступности и конфиденциальности информации и защиты жизненно важных интересов личности, общества и государства в информационной сфере.

Сегодня мы можем констатировать, что в процессе своего развития мировая «информационная» 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, основными задачами которой 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 в области защиты информации.

Рассматривая общее содержание перечисленных задач, мы можем отметить, что в плане организации работ по защите информации в большинстве стран к настоящему времени на государственном уровне созданы достаточно стройные и эффективные системы управляющих органов. В Российской Федерации, например, основу

этой системы составляют такие государственные структуры, как Совет Безопасности, Федеральная служба безопасности, Федеральная служба по техническому и экспортному контролю, Министерство внутренних дел и др.

На уровне объектов информатизации (предприятия и компании различных форм собственности, 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, подходах, методах и средствах ее решения, которые связаны с активным формированием информационного общества, предопределяют необходимость существенной корректировки как организации, так и содержания их деятельности. В частности, расширение рамок комплексности защиты требует укомплектования соответствующих служб кадрами высококвалифицированных специалистов по техническим, организационным, правовым и гуманитарным аспектам защиты информации. 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 особенностью проблемы защиты информации является то, что ее решение должно осуществляться в условиях неопределенности, а зачастую и невозможности прогнозирования проявления отдельных 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 одним из основных способов организационного решения проблемы защиты информации на региональном уровне.

Анализируя доступные нам результаты научных исследований и разработок в области защиты информации, мы можем констатировать, что до последнего времени данные разработки в основном были направлены на развитие технических средств защиты (физических, программно-аппаратных, криптографических). Современный период развития информатизации общества, как это уже отме-

чалось, 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, можно говорить о полномасштабной постановке проблемы обеспечения информационной безопасности как органической совокупности процессов защиты информации и защиты от информации.

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 [3]. 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 при-

оритетное формирование теории защиты информации как краеугольного камня интенсификации процессов обеспечения информационной безопасности.

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 Московском инженерно-физическом институте. 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 [4].

Углубленное изучение проблемы формирования научно-методологического базиса теории защиты информации 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 указанной 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 ее осуществления 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. Дальнейшая задача в этой области заключается в создании чет-

кой государственной системы прогнозирования потребности в специалистах, разработке методологии формирования государственного заказа на подготовку, 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:

- создание теоретических основ защиты информации и формирование научно-методологического базиса, позволяющих адекватно описывать процессы защиты в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов;
- разработка научно обоснованных подходов к формированию нормативно-методических документов по защите информации;
- 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 Доктрины информационной безопасности Российской Федерации, Стратегии развития информационного общества в Российской Федерации и Стратегии национальной безопасности Российской Федерации до 2020 года.

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 перечень проблем, попытка рассмотрения которых предпринята в данной монографии:

- 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;
- формирование общеметодологических принципов построения систем защиты информации и управления процессами их функционирования;
- выработка практических рекомендаций по интенсификации процессов защиты информации и формированию современных организационных структур, обеспечивающих эффективную реализацию комплексного подхода к защите.

Первое и второе из указанных направлений должны быть посвящены рассмотрению общих аспектов проблемы безопасности как научной категории, определению места информационной безопасности в обеспечении национальной безопасности государства. Целью исследований в этом направлении является формулирование современной постановки задачи защиты, суть которой, как следует из предыдущего, состоит в переходе от экстенсивных к интенсивным методам решения проблем.

Далее логично должны рассматриваться научно-методологические основы интенсификации процессов защиты информации, на основе чего может быть сформирован научно-методологический базис решения задач защиты. Очевидно, что на повестку дня при этом встанут проблемы расширения арсенала классической теории систем за счет использования методов, позволяющих адекватно моделировать процессы, существенно зависящие от воздействия трудно предсказуемых факторов, и решать задачи анализа, т. е. оценки защищенности (уязвимости) информации, и синтеза, т. е. оптимизации распределения ресурсов, выделяемых на защиту.

Четвертое направление посвящено решению проблемы количественной оценки угроз защищаемой информации. Первоочередной задачей здесь является разработка системной классификации угроз и формирование модели определения количественных показателей для оценки уязвимости информации.

Следующее направление исследований предусматривает создание рациональной классификации множества вариантов потенциально возможных условий защиты и формирование на этой основе необходимого и достаточного набора типовых систем защиты информации.

Далее решаются вопросы выработки единых методологических принципов создания систем защиты информации и управления

их функционированием на основе широкомасштабной типизации и стандартизации данных систем.

Наконец, последнее из выделенных направлений исследований должно быть нацелено на определение перспектив развития теории и практики защиты информации и формулирование, концепции организационного кадрового обеспечения решения проблем информационной безопасности.

В совокупности указанные проблемы и должны составить ядро формируемого нового научного направления — теории защиты информации.