



ПЕРВАЯ СТАТЬЯ

БИТ

А. А. Малюк

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОВОКУПНОСТИ ИНФОРМАЦИОННЫХ ПРОБЛЕМ СОВРЕМЕННОГО ОБЩЕСТВА

Данная статья является продолжением изложения взглядов автора на современные проблемы защиты информации (см. статью «Защита информации: современные проблемы» (Безопасность информационных технологий. 2010. № 1)). Ее цель — проанализировать роль и место этих проблем в общей совокупности проблем развития информационного общества. Однако прежде чем рассматривать весь спектр данных проблем, целесообразно определить содержание более общего широко используемого в последнее время понятия «информационная безопасность». Тем более что среди специалистов в области обеспечения информационной безопасности в настоящее время нет единства в этом вопросе.

Если рассматривать безопасность в качестве общенаучной категории, то представляется, что она может быть определена как некоторое качество той или иной системы, характеризующее, с одной стороны, ее способность противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой — возможность возникновения и уровень угроз для элементов самой системы и внешней среды, связанных с ее функционированием. При таком определении мерой безопасности системы могут служить:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз — степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии дестабилизирующих факторов;
- с точки зрения отсутствия угроз для элементов самой системы и внешней среды — степень (уровень) возможности (или отсутствие возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам системы или внешней среде.

Чисто механическая интерпретация данных формулировок приводит к следующему определению информационной безопасности:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМЫ — это ее качество, характеризующее, с одной стороны, способность противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой — уровень угроз, которые создает ее функционирование для элементов самой системы и внешней среды.

Такое определение информационной безопасности отличается от положенного в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации (ср.: «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной

сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»). Использование термина «состояние защищенности», на наш взгляд, не учитывает динамики изменений, происходящих в процессе функционирования системы. Понятие же безопасности как качества более объективно характеризует способность противостоять тем или иным угрозам как внешнего, так и внутреннего характера.

Учитывая приведенные соображения, предложенное определение можно считать достаточно полным и вполне корректным. Однако для того, чтобы служить более конкретным ориентиром в направлении поиска путей решения проблем обеспечения информационной безопасности, оно нуждается в уточнении и детализации его основополагающих понятий. При этом отправной точкой может служить тот факт, что информация как непреходящий компонент любой организованной системы, с одной стороны, легко уязвима (т. е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой — сама может быть источником угроз как для элементов системы, так и для внешней среды. Отсюда естественным образом вытекает, что обеспечение информационной безопасности в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех задач:

первая — защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;

вторая — защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз (защита от информации);

третья — защита внешней среды от информационных угроз со стороны рассматриваемой системы (защита от информации).

В соответствии с изложенным, общая схема обеспечения информационной безопасности может быть представлена так, как показано на рис. 1.

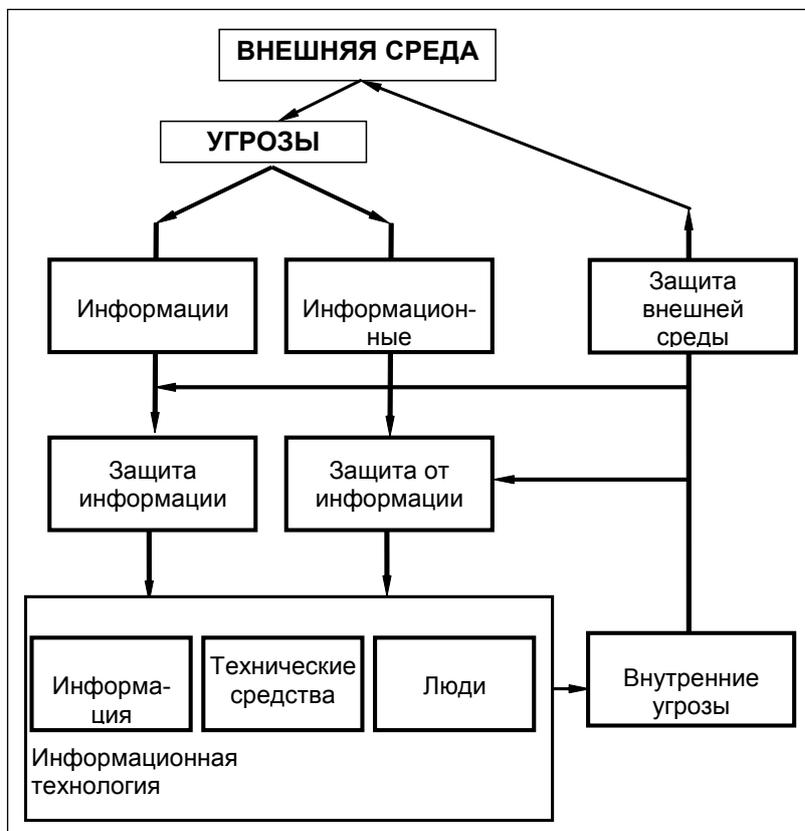


Рис. 1. Общая схема обеспечения информационной безопасности



Естественно, что проблемы обеспечения информационной безопасности входят в состав более общих проблем информатизации. Поэтому их содержание должно формироваться в строгом соответствии с содержанием проблем информатизации, а концептуальные подходы к их решению должны взаимоувязываться с концепциями информатизации.

Представляется, что к основным концептуальным вопросам информатизации, или, другими словами, развития информационного общества, должны быть отнесены:

- сущность информатизации;
- конечные результаты информатизации;
- пути, средства и методы достижения основных результатов информатизации.

Не вдаваясь в философские аспекты формирования информационного общества, а взяв за основу прагматическое значение информатизации, можно с полным основанием утверждать, что ее сущность заключается в формировании такой информационной среды, в которой имелись бы все объективные предпосылки, необходимые для наиболее рационального информационного обеспечения всех сфер деятельности современного общества. Создание такой среды, естественно, предполагает всеобщую компьютеризацию, которую нередко представляют как основную и единственную черту информационного общества. Однако она — лишь компонент (хотя и один из важнейших) формирования общей инфраструктуры информационной среды.

Ключевым же для информационного общества является то, что производство, переработка и использование информации становятся в современных условиях важнейшей отраслью экономики, которая и получила общепризнанное название информационной индустрии. Таким образом, создание объективных предпосылок, необходимых для формирования информационной индустрии, и составляет основное содержание информатизации современного общества. При этом научно-методологическим базисом этого процесса служит информатика.

Перед информатикой фактически стоят две основные задачи: изучение информационных проблем общества и разработка путей, методов и средств наиболее рационального их решения. Изучение информационных проблем поставлено нами на первое место совсем не случайно. Этим однозначно определяется, что такое изучение является базисом для реализации второй основной задачи информатики — разработки путей, методов и средств наиболее рационального решения этих проблем и прежде всего удовлетворения информационных потребностей общества в процессе его жизнедеятельности. Таким образом, пути, методы и средства информатизации должны разрабатываться исходя из информационных потребностей. Однако в связи с явным наличием обратной связи информационные потребности общества должны максимально приспосабливаться к возможностям их удовлетворения. Это означает, что информационные процессы в различных сферах деятельности должны быть целенаправленно подготовлены к переводу их на индустриальные методы осуществления.

Структурированные таким образом информационные потребности общества и являются одной из основных предпосылок для разработки необходимого арсенала методов и средств информатизации. Основу этого арсенала должны составлять унифицированные методы и современные средства обработки информации. На их базе должна разрабатываться концепция индустриализации переработки информации и необходимые для этого информационные технологии.

Объективные предпосылки индустриализации процесса информационного обеспечения различных сторон деятельности современного общества заложены совокупностью важнейших результатов развития информатики за последнее время. К ним, прежде всего, относятся:

- системная классификация информации;
- унификация структуры информационного потока;
- унификация процедур (задач) обработки информации;

- систематизация методов обработки информации;
- унификация информационной технологии;
- формирование концепции управления процессами обработки информации по унифицированной технологии.

Последний из приведенных результатов носит многоаспектный характер, касаясь в качестве одной из основных составляющих проблемы обеспечения информационной безопасности. Современное состояние теоретической и практической разработки этой проблемы может быть оценено следующим образом. Первая ее составляющая, т. е. проблема защиты информации, уже продолжительное время (свыше 40 лет) находится в центре внимания специалистов, и к настоящему времени можно говорить о следующих общепризнанных результатах:

- проблема получила практически всеобщее признание;
- заложены основы разработки теории защиты;
- налажено широкомасштабное производство средств защиты;
- организованы планомерная подготовка и повышение квалификации специалистов соответствующего профиля;
- создана государственная система защиты информации;
- накоплен значительный опыт практического решения задач защиты информации в системах различного масштаба и функционального назначения.

На основе перечисленных результатов справедливым будет утверждение, что защита информации как одна из основных сфер деятельности, присущих информационному обществу, имеет определенный ресурс для дальнейшего целенаправленного развития. При этом основные задачи такого развития на ближайшую перспективу могут быть сформулированы следующим образом.

Первая и самая неотложная — регулярный сбор и обработка статистических данных о составе и результатах функционирования реальных систем защиты. Полученные в ходе такого мониторинга и аудита данные необходимы как для совершенствования методологии проектирования новых систем защиты и повышения эффективности их функционирования, так и для дальнейшего развития теории защиты, поскольку заложенные на сегодняшний день основы носят по преимуществу вербальный характер. Развитая же теория должна содержать количественные методы анализа и синтеза систем защиты и управления ими в процессе функционирования.

Вторая задача заключается в создании организационных структур, обеспечивающих решение первой задачи. Такие организационные структуры могут, например, формироваться в виде специализированных региональных центров защиты, на базе которых можно было бы развернуть эффективную систему сбора и обработки статистических данных, а также обеспечить оказание широкого спектра услуг своим абонентам на основе аутсорсинга информационной безопасности.

Третья задача — это дальнейшее развитие научно-методологического базиса как основы интенсификации процессов защиты. Составными частями данной задачи выступают:

- во-первых, формирование более общей (по сравнению с классической) теории систем, ориентированной не только на технические, но и на социальные системы;
- во-вторых, разработка на основе вербальной теории строгой теории защиты, базисом которой должны служить общая теория систем и статистические данные о структуре и функционировании систем защиты информации, получаемые при решении первой сформулированной задачи;
- в-третьих, разработка комплекса рабочих моделей, необходимых и достаточных для решения всех задач защиты информации.

Рассматривая эти направления в качестве основных на сегодняшний день, мы не можем в то же время, хотя бы вкратце, не остановиться на состоянии дел с изучением и разработкой мер обеспечения второй составляющей информационной безопасности — защиты от информации.



Дело в том, что наблюдаемые в последние годы тенденции в развитии информационных технологий уже практически привели к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, одной из которых является так называемая информационная война.

Защита от информации заключается в использовании специальных методов и средств (в основном организационно-правового и гуманитарного характера) в целях предупреждения или нейтрализации негативного воздействия информации на элементы самой системы, а также предупреждения негативного воздействия выходной информации системы на элементы внешней среды. Данный вид защиты распространяется на информацию, как циркулирующую внутри системы, так и поступающую из внешней среды. Актуальность этой части общей проблемы информационной безопасности заключается в том, что информация способна оказывать такое воздействие на людей и технические комплексы, результаты которого могут носить не просто негативный, а трагический и даже катастрофический характер.

Уже одного этого достаточно для утверждения о чрезвычайной важности проблемы защиты от информации в условиях формирования информационного общества. В то же время, несмотря на практически всеобщее понимание (по крайней мере, среди специалистов) важности проблемы, признание ее в качестве приоритетной на уровне Совета Безопасности Российской Федерации, исследования и разработки в этом направлении на сегодняшний день развернуты слабо и практически не финансируются.

Справедливости ради надо отметить, что проблема защиты от информации существенно сложнее проблемы защиты информации в силу того, что информационные угрозы чрезвычайно многообразны, а их воздействие далеко не всегда очевидно. Предотвращение и нейтрализация информационных угроз требуют не столько технических, сколько организационно-правовых и политических решений, причем не только на внутригосударственном, но и на международном уровне.

В постановочном плане представляется, что задача защиты от информации естественным образом делится на две составляющие: защита от информации технических средств и систем и аналогичная защита людей.

Наш анализ показывает, что применительно к первой составляющей, т. е. к защите от информации технических средств и систем, основные положения развиваемой в последнее время концепции комплексной защиты информации остаются адекватными без особой трансформации (с точностью до нюансов терминов). Что же касается защиты от информации людей, то здесь эта адекватность не является такой очевидной в силу широкого и разнопланового воздействия на них информации и разномасштабности постановки задачи обеспечения информационной безопасности.

Отличительная особенность проблемы защиты людей от информации, создающая дополнительные трудности, состоит в том, что ее решение носит преимущественно гуманитарный характер, в то время как решения по защите от информации технических средств и систем, так же как и по защите информации, имеют существенную техническую составляющую и в основном поддаются строгой структуризации.