ИНФОРМАЦИОННАЯ ВОЙНА И СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Малюк А. А.[1]

DOI: 10.21681/2311-3456-2024-5-105-114

Аннотация. *Появление данной статьи является следствием бурного развития в последнее время средств и технологий ведения информационной войны, практического превращения ее в основную форму военно-силового противоборства в XXI веке. В связи с этим особую остроту приобретает задача разработки концептуальных и методологических подходов к формированию комплексной системы обеспечения информационной безопасности, учитывающей принципиально междисциплинарный характер этого вида деятельности и необходимость принятия решений в условиях неполноты и недостоверности исходной информации. Под этим углом в статье предлагается рассматривать обеспечение информационной безопасности как совокупность процессов защиты информации и защиты от информации, что приводит к новым подходам к разработке соответствующих нормативно-методических документов и рационализации схем и структур управления комплексной защитой на объектовом, региональном и государственном уровнях.*

Ключевые слова: *информационная война, информационная безопасность, защита информации, защита от информации, комплексное обеспечение информационной безопасности, культура информационной безопасности.*

Введение

Постоянно расширяющееся использование новых информационных технологий привело мировую цивилизацию к формированию нового информационного общества. Сегодня все мы являемся свидетелями серьезнейших качественных изменений в экономической, социально-политической и духовной сферах общественной жизни. При этом необходимо констатировать, что 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, причем и на межгосударственном уровне [1,2].

В связи с этим важнейшее значение в настоящее время приобретает задача обеспечения информационной безопасности (ИБ) как органической совокупности решения задач защиты информации и защиты от информации. Все это говорит о необходимости формирования научно-методологического базиса такой комплексной защиты как краеугольного камня интенсификации процессов обеспечения информационной безопасности. В подтверждение такой постановки проблемы можно сослаться на Доктрину информационной безопасности Российской Федерации, утвержденную Президентом страны в декабре 2016 года (Указ от 05.12.2016, № 646), которая констатирует, что «информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности России». В Доктрине прямо указывается, что «обеспечение информационной безопасности играет ключевую роль в обеспечении национальной безопасности страны».

И отечественные, и зарубежные специалисты единодушны в оценке чрезвычайной важности проблемы обеспечения ИБ, история которой насчитывает уже практически полвека. Естественно, что за истекшее после возникновения проблемы время коренным образом изменилось как представление о ее сущности, так и методологические подходы к решению. Как уже отмечалось, характерный для настоящего времени этап с полным правом может быть назван этапом комплексной защиты. Его особенность заключается в попытках обобщения всего имеющегося опыта теоретических исследований и практического решения задач обеспечения ИБ. Основная задача переживаемого этапа – перевод всего дела обеспечения ИБ на интенсивные способы, базирующиеся на строгой научной основе.

1 Малюк Анатолий Александрович, кандидат технических наук, профессор, Заслуженный работник высшей школы РФ, профессор кафедры криптологии и кибербезопасности (№42) НИЯУ МИФИ, Москва, Россия. E-mail: AAMalyuk@mephi.ru

Углубленное изучение проблемы формирования научно-методологического базиса теории защиты информации привело к выводу, что эффективное решение задач защиты возможно только с учетом органической взаимосвязи 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.

Таким образом, представляется, что основная цель и направленность научных исследований в области обеспечения информационной безопасности заключается сегодня в разработке концептуальных и методологических подходов к интенсификации процессов защиты информации и защиты от информации, позволяющих усовершенствовать организацию систем защиты и управление их функционированием.

Информационная война как средство военно-силового противоборства

Исторический анализ тенденций в развитии военно-силового противоборства ясно показывает, что «информационные войны» практически превращаются в основное средство борьбы в XXI веке [3,4]. И этот процесс благодаря чрезвычайно высокой информационной зависимости всех сфер жизнедеятельности современного общества будет продолжаться со все возрастающей скоростью. Информационная война становится очень эффективным средством нанесения непоправимого ущерба «противнику», а «информационное оружие» начинает представлять все более серьезную военную угрозу.

В подтверждение этого можно привести оценку американских экспертов, утверждающих, что нарушение работы компьютерных сетей, используемых в системах управления государственными и банковскими структурами США, путем вывода из строя вычислительных и связных средств или уничтожения хранящейся в сетях информации способно нанести экономике страны настолько серьезный ущерб, что его можно сравнивать с ущербом от применения против США ядерного оружия[2].

Если говорить о негативном воздействии информации на личность и общество и необходимости применять в этом случае соответствующие меры защиты, то можно констатировать, что эта проблема имеет, вообще говоря, глубокие исторические корни. В качестве примера здесь можно привести Указ Императрицы Елизаветы Петровны[3], относящийся к XVIII веку. Дословно:

«Мы с крайним неудовольствием уведомились, что многие как из наших подданных, так и живущих здесь в нашей службе и в нашей протекции иностранцев, разглашая многие лживые ведомости о нынешних статских, политических и воинских делах, присовокупляя к тому развратные толкования и совсем нескладные рассуждения, с столь большею продерзостью, сколь меньшее об оных имеют они сведение и понятие; и для того запотребно рассудили мы чрез сие для известия каждого объявить: что ежели кто отныне, разглашая какие-либо известия или еще и вымышляя оные, о не принадлежащих до него особливо политических и воинских делах превратные толкования и рассуждения делать станет, а нам о том донесется, такой неминуемо всю тягость нашего гнева почувствует».

Сегодня можно выделить целый ряд основных объектов, как технического, так и социально-психологического характера, уязвимых с точки зрения вредного воздействия информации и нуждающихся в применении тех или иных средств защиты. К таким объектам относятся:

- военная информационная инфраструктура, решающая в интересах вооруженных сил задачи управления войсками и боевыми средствами, сбора и обработки информации;
- критическая информационная инфраструктура, объединяющая государственное управление, управленческие структуры кредитно-финансовой сферы, транспортных и промышленных предприятий;
- средства массовой информации, в первую очередь электронные (радио, телевидение, Интернет и т.д.);
- психологические ресурсы общества (система ценностей, индивидуальное и массовое сознание граждан, их психическое здоровье).

В последнее время значительно увеличилось число различных публикаций, посвященных таким вопросам как цели и последствия информационной войны, особенности и виды информационных войн, особенности применения информационно-технического оружия при ведении современных гибридных войн, информационные войны как результат социального управления и социального взаимодействия в эпоху глобализации, влияние информационных войн на стабильность государства, особенности ведения современных информационных войн в средствах массовой информации (СМИ) и в сети Интернет, социальные сети как инструмент ведения информационных войн, феномен так называемых «фейк-новостей» в современной информационной войне и др.

2 По материалам средств массовой информации.
3 Газета «С. Петербургские ведомости», 1750 г., № 46.

Основной вывод из анализа этих публикаций заключается в том, что сегодня проблема защиты от информационного оружия заслуживает самого пристального внимания. Дело в том, что, например, по данным ЦРУ США, число стран, разрабатывающих сегодня информационное оружие (в основном с использованием сети Интернет), превышает 120 (при 30, разрабатывающих оружие массового уничтожения), и рано или поздно они получат возможность вести информационные войны. Основными задачами в них, очевидно, будут дезорганизация функционирования критически важных военных, промышленных, административных объектов и систем «противника», а также информационно-психологическое воздействие на военно-политическое руководство, войска и население.

Каковы же основные цели информационной войны? Следуя тому, о чем уже говорилось, напрашивается заключение, что этими целями могут быть:

- дезорганизация деятельности управленческих структур, транспортных потоков и средств коммуникации;
- блокирование деятельности отдельных предприятий и банков, а также целых отраслей промышленности путем нарушения многозвенных технологических связей и системы взаиморасчетов, проведения валютно-финансовых махинаций и т.п.;
- инициирование крупных техногенных катастроф на территории «противника» в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;
- массовое распространение и внедрение в сознание людей определенных представлений, привычек и поведенческих стереотипов;
- вызов недовольства или паники среди населения, а также провоцирование деструктивных действий различных социальных групп.

При этом объектом информационного противоборства может явиться любой объект, в отношении которого возможно осуществление информационного воздействия, результатом чего будет модификация его свойств как системы (информационной, экономической, политической и т.д.). Таким образом, ясно, что объектом информационного противоборства может стать любой сегмент информационно-психологического пространства, в том числе массовое и индивидуальное сознание граждан, социально-политические системы и процессы, информационная инфраструктура, информационные и психологические ресурсы.

Определив объекты информационного противоборства, необходимо определить и субъекты, которые могут применять информационное оружие. Сюда могут быть отнесены:

- государства, их союзы и коалиции;
- международные организации;
- негосударственные (в том числе – незаконные) вооруженные формирования и организации террористической, экстремистской, радикальной политической и религиозной направленности;
- транснациональные корпорации;
- виртуальные социальные сообщества;
- медиа-корпорации;
- виртуальные коалиции.

Все приведенные субъекты в этом случае должны обладать вполне определенными признаками, которые предполагают их заинтересованность и возможность осуществлять информационное противоборство. К этим признакам могут быть отнесены:

- наличие у субъекта в информационно-психологическом пространстве собственных интересов;
- наличие в составе субъекта специальных сил (структур), функционально предназначенных для ведения информационного противоборства или уполномоченных на его ведение;
- обладание информационным оружием или его разработка, а также разработка средств его доставки и маскировки;
- наличие под контролем субъекта определенного сегмента информационного пространства, в пределах которого он обладает преимущественным правом устанавливать нормы регулирования информационно-психологических отношений (на правах собственности, закрепленных нормами национального и международного законодательства) или государственным суверенитетом;
- существование в официальной идеологии положений, допускающих участие субъекта в информационном противоборстве.

Здесь целесообразно особо выделить роль в информационно-психологической борьбе транснациональных сетевых корпораций, которую можно охарактеризовать следующим образом.

Первое, транснациональные корпорации в глобальном информационном обществе практически обладают всеми признаками суверенного государства – территорией, определяемой ареалом распространения их сетевой инфраструктуры, стратегическими ресурсами (информационными потоками в их информационных и телекоммуникационных системах), «населением» (штатом сотрудников) и относительно полным суверенитетом.

DOI: 10.21681/2311-3456-2024-5-105-114

И второе, транснациональные корпорации, разрабатывая новые информационно-коммуникационные технологии, развивая свои информационные и телекоммуникационные системы и сети, контролируя циркулирующие по ним потоки, создают театр военных действий, на котором затем будут разворачиваться боевые действия между участниками информационно-психологического противоборства.

Итак, из проведенного нами краткого анализа военных и международных аспектов проблемы информационной войны можно сделать сегодня следующие основные выводы:

- ряд стран стремится получить преимущество в создании систем и средств ведения информационной войны, что представляло бы серьезную угрозу национальной безопасности России;
- создание целостного комплекса средств и методов ведения информационной войны будет осуществляться постепенно, по мере развития в мире базовых информационных технологий, что позволяет осуществлять мониторинг этого процесса;
- тема информационного оружия и информационной войны, в силу своей чрезвычайной важности для безопасности страны, требует комплексной проработки ее военно-стратегических, правовых, разведывательных и контрразведывательных аспектов, а также координации усилий всех заинтересованных ведомств России.

Общие аспекты проблемы безопасности как научной категории, подходы к обеспечению информационной безопасности

Прежде чем рассматривать проблемы, связанные с обеспечением информационной безопасности, целесообразно, наверное, определить содержание общего понятия «безопасность», тем более что среди специалистов в этой области единство в настоящее время практически отсутствует. Разработка общей теории безопасности (или, как принято называть ее сегодня, «секьюритологии») пока не нашла своего удовлетворительного разрешения, хотя, по мнению большинства ученых, формирование этого нового научного направления является важнейшим условием выживания и развития человечества. Пока по-прежнему многие базовые понятия и определения этого направления («безопасность», «опасность», «угроза безопасности», «виды безопасности» и др.) носят дискуссионный характер. При этом отметим, что если говорить о рассматриваемом нами предмете «информационная безопасность», то многие определения ИБ, которые хотя и могут быть приняты в плане практическом, не отражают специфики современного этапа формирования информационного общества.

Если рассматривать безопасность как общенаучную категорию, 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 подходе мерой безопасности системы, очевидно, 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 отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам системы или внешней среде.

Интерпретация данного подхода в области ИБ приводит нас к следующему возможному определению.

Информационная безопасность системы – это ее качество, характеризующее, с одной стороны, способность противостоять дестабилизирующему воздействию внешних и внутренних угроз информации, а с другой – уровень информационных угроз, которые создает ее функционирование для элементов самой системы и внешней среды.

Как видим, такое определение ИБ отличается от определения, положенного в основу Доктрины информационной безопасности Российской Федерации. Представляется, что использование термина «состояние защищенности» не учитывает происходящих в последнее время изменений в подходах к созданию новых информационных технологий (например, технологии облачных вычислений). При этом безопасность должна рассматриваться не как некоторая надстройка, обеспечивающая «состояние защищенности», а как изначальный базис технологии, т.е. ее непременное «качество». Таким образом, представление безопасности как качества более объективно характеризует способность системы противостоять тем или иным угрозам как внешнего, так и внутреннего характера.

Учитывая это, приведенное нами определение можно считать более полным и достаточно корректным. Вместе с тем, чтобы сделать его ориентиром при поиске решения проблемы обеспечения ИБ, необходимо уточнение и детализация его основополагающих понятий. В качестве отправной точки

такого уточнения используем тот факт, что информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима, а с другой сама может быть источником угроз, как для элементов самой системы, так и для внешней среды. Отсюда естественным образом вытекает, что обеспечение ИБ в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении двух задач (подтвердим это еще раз):

- ***защита информации***, под которой понимается защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз;
- ***защита от информации***, подразумевающая защиту элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз, а также защиту внешней среды от информационных угроз со стороны рассматриваемой нами системы.

Еще одно важное, на наш взгляд, замечание. Проблема обеспечения ИБ является составляющей более общих проблем информатизации. Поэтому ее содержание должно формироваться в строгом соответствии с содержанием проблем информатизации, а концептуальные подходы к ее решению должны быть взаимоувязаны с концепциями информатизации.

Остановимся далее на современном состоянии теоретической и практической разработки проблемы обеспечения ИБ. Первая ее составляющая, т.е. проблема защиты информации, уже продолжительное время (свыше 40 лет) находится в центре внимания специалистов, и к настоящему времени на примере Российской Федерации можно говорить о следующих общепризнанных результатах:

- в настоящее время практически разработаны основы теории защиты информации;
- налажено широкомасштабное производство технических и программных средств защиты;
- создана целостная государственная система защиты информации;
- организована планомерная подготовка и повышение квалификации специалистов соответствующего уровня и профиля;
- накоплен значительный опыт практического решения задач защиты информации в системах различного масштаба и функционального назначения.

На основе перечисленных результатов можно констатировать, что защита информации сегодня имеет определенный базис для дальнейшего целенаправленного развития. При этом, основные задачи такого развития на ближайшую перспективу могут быть сформулированы следующим образом:

- организация регулярного сбора и обработки статистических данных о составе и результатах функционирования реальных систем защиты, которые необходимы для совершенствования методологии проектирования новых систем защиты, повышения эффективности их функционирования, дальнейшего развития теории защиты;
- создание организационных структур, обеспечивающих решение первой задачи, которые, как показывает накопленный на сегодня опыт, могут, например, формироваться в виде специализированных региональных и отраслевых центров защиты, способных обеспечить оказание широкого спектра услуг своим абонентам;
- дальнейшее развитие научно-методологического базиса как основы интенсификации процессов защиты.

Решение последней задачи, очевидно, включает следующие проблемы:

- формирование более общей (по сравнению с классической) теории систем, ориентированной не только на технические, но и на социальные системы;
- разработка строгой аксиоматической теории защиты информации, базисом которой должны служить общая теория систем и статистические данные о структуре и функционировании реальных систем защиты;
- разработка комплекса рабочих моделей, необходимых и достаточных для решения всей совокупности задач защиты информации.

Обратимся далее к состоянию дел с изучением и разработкой мер обеспечения второй составляющей ИБ – защиты от информации. При этом обратим внимание на то, что информация способна оказывать такое воздействие как на технические комплексы, так и на людей, результаты которого могут носить не просто негативный, а трагический и даже катастрофический характер. Все это свидетельствует о чрезвычайной важности проблемы защиты от информации в условиях формирования информационного общества. Причем, необходимо 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.

В постановочном плане задача защиты от информации естественным образом делится на две составляющие: защита от информации технических средств и систем и аналогичная защита людей. Если говорить о первой составляющей, т.е. защите от информации технических средств и систем, то можно констатировать, что основные положения развиваемой

в последнее время концепции комплексной защиты информации остаются здесь вполне адекватными (с точностью до нюансов терминов). Предотвращение же и нейтрализация информационных угроз, направленных на людей, требуют не столько технических решений, сколько организационно-правовых и политических, причем не только на внутригосударственном, но и на международном уровне.

Таким образом, отличительная особенность проблемы защиты людей от информации, создающая, кстати, немалые 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 имеют существенную техническую составляющую и, в основном, поддаются строгой структуризации.

Современная постановка задач защиты информации и защиты от информации

Для обеспечения информационной безопасности, как следует из предыдущего изложения, необходимо решение двух задач – защиты информации и защиты от информации.

Если говорить о первой из них, то необходимо отметить, что в современных условиях существуют и объективная необходимость, и объективные предпосылки для кардинального изменения взгляда на саму проблему защиты информации и подходы к ее решению. Заметим, что необходимость своевременного видоизменения постановки задачи является одним из важнейших общеметодологических принципов развития науки.

Основные факторы, обуславливающие объективную необходимость назревшего изменения постановки задачи защиты, заключаются в следующем.

1. ***Исключительное повышение значимости информации как общественного ресурса***. Отметим, что главным противоречием современного информационного общества является как бы «индустриальный» характер современных информационных технологий, с одной стороны, и сохраненный со времен индустриального общества характер управления им, существенно зависящий от искусства управленческого персонала. В целях преодоления названного противоречия управление должно быть основано на других принципах, как бы использующих методы поточно-индустриального производства. Осуществление такого перевода и составляет одну из главных задач развития информационного общества. А поскольку всякое управление в основе своей есть информационный процесс, то это еще раз подтверждает тот факт, что информация приобретает сегодня статус главного ресурса общества со всеми вытекающими из этого требованиями, предъявляемыми к обращению с ним.
2. ***Существенные изменения в организации информационных технологий***. Современные информационные технологии характеризуются массовым насыщением сверхбыстродействующими компьютерными средствами и объединением их в глобальные сети, что обеспечивает расширение обработки огромных объемов информации в очень короткие сроки, не достижимые на предыдущих этапах общественного развития.
3. ***Все возрастающие опасности злоумышленных действий по отношению к информации и злоумышленного ее использования***. Настоящее время характеризуется исключительным ростом преступности, использующей возможности информационно-коммуникационных технологий для нанесения ущерба интересам граждан, общества и государства. При этом возможности злоумышленного использования информации достигли такого уровня, что сегодня, как уже отмечалось выше, практически ведутся информационные войны.

Решить возникающие в этих условиях проблемы можно только видоизменив саму постановку задачи защиты информации. Успех в этом могут обеспечить следующие обстоятельства.

1. ***Наличие богатого опыта организации различных защитных процессов по отношению к информации как в традиционных («бумажных»), так и в автоматизированных технологиях ее обработки***. На сегодняшний день отработаны современные методологии обеспечения сохранности (целостности) информации, ее надежности, качества обработки и выдачи, регулирования использования (предупреждения несанкционированного доступа).
2. ***Значительные достижения в научном обеспечении названных выше процессов***. В последние два десятилетия XX века большое развитие получили теория надежности [5–7] и теория обеспечения качества информации [8]. В настоящий момент можно также с уверенностью утверждать, что разработаны основы теории защиты информации (в первую очередь трудами отечественных ученых).
3. ***Возможности решения всех проблем организации защитных процессов по отношению к информации в рамках единой концепции***. Такой концепцией может стать разрабатываемая в теории защиты информации унифицированная концепция защиты [9,10].

Таким образом, видоизмененная постановка задачи защиты информации должна учитывать

совокупность следующих основных концептуальных положений:

- интегральное представление понятия комплексности защиты информации в целевом и инструментальном планах;
- расширение рамок защиты от обеспечения компьютерной безопасности до защиты информации на объекте и защиты информационных ресурсов региона и государства;
- комплексное организационное построение систем защиты информации;
- обеспечение условий наиболее эффективного использования информации;
- переход к так называемой упреждающей стратегии осуществления защитных процессов.

Фактически при таком подходе проблема защиты информации как бы перерастает в более общую проблему управления информационными ресурсами.

Помимо защиты информации важнейшей составляющей обеспечения информационной безопасности является защита от информации, т.е. защита автоматизированных систем и людей (отдельно взятого человека, коллектива людей, населения региона или государства в целом) от разрушающего воздействия информации. Однако, разработка системно-концептуальных подходов к решению этой проблемы находится сегодня на начальной стадии. Объективная причина такого положения заключается в необычности проблемы, чрезвычайной ее сложности, многоаспектности и высоком уровне неопределенности. Существует и субъективная причина, заключающаяся в отсутствии до последнего времени общегосударственной востребованности серьезного решения этой проблемы. В средствах массовой информации время от времени появляются публикации по отдельным вопросам и конкретным фактам злоумышленного использования информации как средства противоборства при силовом решении политических, социальных и экономических проблем. Однако системные теоретико-концептуальные исследования проблемы защиты от информации еще ждут своего осуществления. Представляется, что положение здесь должно существенно улучшиться в связи с реализацией Стратегии развития информационного общества и Доктрины информационной безопасности Российской Федерации.

Выше мы уже упоминали о возможности трансформации в этих целях основных положений УКЗИ и использования их для решения задачи защиты от вредной информации различного рода автоматизированных систем. Действительно, основанием такого вывода служат сравнительно тесная родственная связь обеих задач и высокий уровень проработки и научной обоснованности УКЗИ. Как показывает практика использования основных положений УКЗИ при создании реальных систем защиты информации, она применима для обеспечения эффективной защиты в любых автоматизированных системах, в том числе организационно-технологического типа, на всех трех уровнях защиты: компьютерном, объектовом, региональном (государственном). На этой основе может быть сделан фундаментальный вывод о том, что полномасштабная реализация УКЗИ является основной частью задачи защиты от информации автоматизированных систем.

Если говорить о второй части информационной войны – негативном воздействии на человека (общество или отдельную личность), то при формулировании задачи защиты от информации в этом случае, естественно, возникает вопрос: каковы же возможности противостоять такому информационному воздействию?

Помимо технологических средств защиты информации и обеспечения информационной безопасности (противодействия так называемым киберугрозам), которые, конечно, и в этом случае имеют существенное значение, важнейшая роль должна отводиться здесь готовности общества к информационному противоборству и способности его противостоять различного рода манипуляциям общественным и личным сознанием граждан. Речь идет о своего рода психологических ресурсах общества, под которыми следует понимать систему ценностей общества и ее устойчивость по отношению к внешним или внутренним деструктивным воздействиям, индивидуальное и массовое сознание граждан и его устойчивость к манипулятивному воздействию и вовлечению в противоправную деятельность различными методами тайного принуждения личности. Наконец, к психологическим ресурсам должно быть отнесено также психическое здоровье граждан и его устойчивость по отношению к внешним или внутренним деструктивным воздействиям. Все это может быть представлено как развитие психологических ресурсов общества. Таким образом, в содержательном плане задача защиты от информации должна в современных условиях включать такие элементы как повышение уровня образования членов информационного общества и формирование культуры информационной безопасности.

Необходимость, пути и условия перехода к интенсивным способам обеспечения информационной безопасности

Под интенсификацией обычно понимается увеличение интенсивности и повышение производительности каких-либо действий, опирающееся, прежде всего, на достижения научно-технического прогресса. С уверенностью можно констатировать, что это довольно характерно для процессов, происходящих

в последнее время в области обеспечения информационной безопасности. При этом, если говорить о первой составляющей – защите информации, то преобладавший здесь до недавнего прошлого подход с полным основанием может быть назван экстенсивным, опирающимся на независимую организацию защиты на каждом объекте информатизации. В противоположность ему, интенсивный подход, являющийся предметом нашего рассмотрения, предполагает организацию защиты информации в соответствии с некоторой единой, научно обоснованной концепцией в масштабах региона и государства в целом.

Таким образом, переход к интенсивным способам защиты означает целенаправленную реализацию всех достижений теории и практики, которые, как мы это уже отмечали, в концентрированном виде отражены в унифицированной концепции защиты информации. С сегодняшних позиций можно выделить ряд основных положений УКЗИ, практическая реализация которых и будет означать переход к интенсивным способам защиты, причем как информации, так и от информации. К этим положениям могут быть отнесены следующие.

1. ***Структурированное описание среды защиты***. Такое описание позволяет четко представить структуру защищаемого объекта или системы и применяемую технологию обработки информации. При этом удобно в целях унификации методов такого описания ввести понятия типового структурного компонента и его типового состояния.
2. ***Количественный анализ степени уязвимости информации***. Такой анализ необходим для объективной оценки реальных угроз информации, принимаемых усилий и расходов на ее защиту. Отметим, что в основах теории защиты информации разработана довольно развитая методология оценки уязвимости информации, состоящая из трех элементов: системы показателей уязвимости, системы угроз информации и системы моделей определения текущих и прогнозирования ожидаемых значений показателей уязвимости.
3. ***Научно обоснованное определение требуемого уровня защиты***. Объективные трудности решения этой задачи связаны с тем, что на уровень защиты как информации, так и от информации в рамках конкретных объектов и условий их функционирования оказывает влияние большое количество разноплановых факторов. При этом, количественное определение требуемого уровня защиты должно быть основано на структуризации всех влияющих на него факторов и их количественных оценках.

Таким образом, интенсификация процессов защиты на основе единой методологии должна, в конечном счете, обеспечить построение оптимальных систем защиты с количественными оценками получаемых решений. При этом оптимизация систем защиты возможна в двух постановках, либо как обеспечение максимально возможного уровня защиты при имеющихся ресурсах, либо как обеспечение требуемого уровня защиты при минимальном расходовании ресурсов. Следует отметить, что для достижения указанных целей может быть использован как бы кортеж концептуальных решений, представляющий собой следующую последовательность: функции защиты – задачи защиты – средства защиты – система защиты. Дадим определения этих элементов кортежа:

- ***функция защиты*** – совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в защищаемой системе различными способами и методами, с целью создания, поддержания и обеспечения условий, объективно необходимых для ее надежной защиты (причем, как информации, обрабатываемой в системе, так и от вредной информации, нарушающей ее работу);
- ***задача защиты*** – организованные возможности средств, методов и мероприятий, осуществляемых в защищаемой системе с целью полной или частичной реализации одной или нескольких функций защиты;
- ***система зашиты*** – организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в защищаемой системе для решения в ней выбранных задач защиты.

Кортеж концептуальных решений создает основу для синтеза оптимальных систем защиты информации с количественными оценками достигаемого уровня защиты. Однако, необходимо отметить ряд трудностей, возникающих при их практической реализации. Наиболее серьезной проблемой здесь является формирование баз исходных данных, необходимых для реализации моделей систем и процессов защиты. Задача эта весьма трудоемкая, да к тому же не может быть решена на основе формальных методов. О трудоемкости задачи можно судить хотя бы по количеству данных, которые надо определять. Это количество оценивается даже для несложных систем числом в несколько тысяч.

Трудности формирования указанных баз исходных данных помимо большого их объема усугубляются еще и весьма высоким уровнем неопределенности, связанной с непредсказуемостью поведения злоумышленников. Исследования данного аспекта проблемы в процессе формирования теории защиты

информации на сегодняшний день привели к выводу, что единственным возможным способом формирования исходных данных является использование неформально-эвристических методов (или другими словами различных видов экспертных оценок). Кроме того, непрерывное изменение условий защиты, постоянный рост возможностей злоумышленного доступа к защищаемой информации, а также совершенствование методов ее защиты требуют того, чтобы экспертные оценки были не просто перманентными, а практически непрерывными. Этого можно достичь лишь при наличии стройной и целенаправленной организации сопровождения работ по защите. Наиболее полным и наиболее адекватным решением этой проблемы было бы создание сети специализированных центров защиты информации (ЦЗИ), аккумулирующих все новейшие достижения в области защиты и специализирующихся на формировании научно-методологического и инструментального базиса решения соответствующих задач на интенсивной основе (включая и базы необходимых исходных данных). Концепция создания и организации работы ЦЗИ к настоящему времени разработана достаточно полно [11,12]. Отметим, что в соответствии с этой концепцией на сегодняшний день в системе высшей школы, например, на базе ряда ведущих вузов уже созданы 29 региональных учебно-научных центров.

В заключение обратим внимание еще на одно весьма важное обстоятельство. Нетрудно видеть, что перевод процессов защиты информации и защиты от информации на интенсивные способы нуждается также в организации эффективной системы кадрового обеспечения информационной безопасности.

Литература

1. *Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В. А.Садовничего и В. П.Шерстюка. – М.: МЦНМО, 2002;*
2. *Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Горячая линия – Телеком, 2003.*
3. *Расторгуев С. П. Философия информационной войны. – М.: Вузовская книга, МПСИ, 2003.*
4. *Ламинина О. Г. Информационные войны: миф или реальность? // Гуманитарные ведомости Тульского государственного педагогического университета им. Л. Н. Толстого (сетевое издание), 2018, №1 (25).*
5. *Дружинин Г. В. Надежность автоматизированных систем. – М.: Энергия, 1997.*
6. *Самойленко С. И., Давыдов Д. А., Золотарев В. В., Третьякова В. Н. Вычислительные сети (адаптивность, помехоустойчивость, надежность). – М.: Наука, 1981.*
7. *Пивоваров А. Н. Методы обеспечения достоверности информации в АСУ. – М.: Радио и связь, 1982.*
8. *Герасименко В. А. Основы управления качеством информации. – М.: Московский историко-архивный институт, 1989, деп. В ВИНИТИ 26.06 89, №5392В89.*
9. *Герасименко В. А., Малюк А. А. Основы защиты информации: Учебник. – М.: МИФИ, 1997.*
10. *Малюк А. А. Теория защиты информации. – М.: Горячая линия–Телеком, 2012.*
11. *Проблемы создания и организации работы центров защиты информации /под ред. А. А.Малюка. // Безопасность информационных технологий, № 4, 1997.*
12. *Малюк А. А., Поляков А. А. Региональные учебно-научные центры по проблемам информационной безопасности – организационная основа реализации положений Доктрины информационной безопасности Российской Федерации в системе высшей школы. // Материалы VIII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», Москва, 2001.*

INFORMATION WARFARE AND MODERN PROBLEMS OF INFORMATION SECURITY

Malyuk A. A.[4]

Abstract. *The appearance of this article is a consequence of the rapid development of means and technologies of information warfare in recent years, its practical transformation into the main form of military-force confrontation in the 21st century. In this regard, the task of developing conceptual and methodological approaches to the formation of an integrated information security system that takes into account the fundamentally interdisciplinary nature of this type of activity and the need to make decisions in conditions of incompleteness and unreliability of initial information is becoming particularly acute. From this point of view, the article proposes to consider information security as a set of processes of information protection and protection against information, which leads to new approaches to the development of relevant regulatory and methodological documents and rationalization of schemes and structures for managing integrated protection at the object, regional and state levels.*

Keywords: *information war, information security, information protection, protection from information, integrated information security, culture of information security.*

4 Anatoly A. Malyuk, Ph.D. (in Tech.), , Professor, Honored Worker of Higher Education of the Russian Federation, Professor of the Department of Cryptology and Cybersecurity (No42) of the National Research Nuclear University MEPhI, Moscow, Russia. E-mail: AAMalyuk@mephi.ru

References

1. *Strel'cov A. A. Obespechenie informacionnoj bezopasnosti Rossii. Teoreticheskie i metodologicheskie osnovy / Pod red. V. A. Sadovnichego i V. P. Sherstjuka. – M.: MCNMO, 2002;*
2. *Manojlo A. V., Petrenko A. I., Frolov D. B. Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny. – M.: Gorjachaja linija – Telekom, 2003.*
3. *Rastorguev S. P. Filosofija informacionnoj vojny. – M.: Vuzovskaja kniga, MPSI, 2003.*
4. *Laminina O. G. Informacionnye vojny: mif ili real'nost'? // Gumanitarnye vedomosti Tul'skogo gosudarstvennogo pedagogicheskogo universiteta im. L. N. Tolstogo (setevoe izdanie), 2018, №1 (25).*
5. *Druzhinin G. V. Nadezhnost' avtomatizirovannyh sistem. – M.: Jenergija, 1997.*
6. *Samojlenko S. I., Davydov D. A., Zolotarev V. V., Tret'jakova V. N. Vychislitel'nye seti (adaptivnost', pomehoustojchivost', nadezhnost'). – M.: Nauka, 1981.*
7. *Pivovarov A. N. Metody obespechenija dostovernosti informacii v ASU. – M.: Radio i svjaz', 1982.*
8. *Gerasimenko V. A. Osnovy upravlenija kachestvom informacii. – M.: Moskovskij istoriko-arhivnyj institut, 1989, dep. V VINITI 26.06 89, №5392B89.*
9. *Gerasimenko V. A., Maljuk A. A. Osnovy zashhity informacii: Uchebnik. – M.: MIFI, 1997.*
10. *Maljuk A. A. Teorija zashhity informacii. – M.: Gorjachaja linija–Telekom, 2012.*
11. *Problemy sozdanija i organizacii raboty centrov zashhity informacii /pod red. A. A.Maljuka // Bezopasnost' informacionnyh tehnologij, № 4,1997.*
12. *Maljuk A. A., Poljakov A. A. Regional'nye uchebno-nauchnye centry po problemam informacionnoj bezopasnosti – organizacionnaja osnova realizacii polozhenij Doktriny informacionnoj bezopasnosti Rossijskoj Federacii v sisteme vysshej shkoly. // Materialy VIII Vserossijskoj nauchno-prakticheskoj konferencii «Problemy informacionnoj bezopasnosti v sisteme vysshej shkoly», Moskva, 2001.*