**1. Основные категории информационной безопасности**

Концептуальные и научно-методологические основы информационной безопасности еще только начинают разрабатываться. Первоочередной задачей при создании теории информационной безопасности следует считать формирование понятийного аппарата. Базовыми понятиями являются информационная опасность, информационная угроза и информационная безопасность.

**Информационная опасность** определяется двояко:

• как состояние окружающей среды или объекта, в котором существует возможность причинить им существенный ущерб или вред путем оказания воздействия на информационную сферу объекта;

• как свойство объекта, характеризующееся способностью наносить существенный ущерб другому объекту путем оказания воздействия на его информационную сферу.

В соответствии с этим **информационная безопасность** – это:

состояние объекта, когда ему путем воздействия на его информационную сферу не может быть нанесен существенный ущерб или вред;

• свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путем оказания воздействия на информационную сферу этого объекта.

**Информационная угроза** – угроза объекту путем оказания воздействия на его информационную сферу:

• намерение нанести (причинить) объекту существенный ущерб путем оказания воздействия на его информационную сферу;

• информационная опасность, реализация которой становится весьма вероятной;

• фактор или совокупность факторов, создающих информационную опасность объекту; такими факторами могут быть действия, поведение объектов, природные явления и т. д.

Все вышесказанное позволяет сформулировать понятие **информационной безопасности Российской Федерации** как такое состояние страны, в котором гражданам, объединениям и общественным группам граждан, обществу и государству не может быть нанесен существенный ущерб путем оказания воздействия на ее информационную сферу.

Основными *объектами информационной безопасности* являются личность (ее права и свободы), общество (его материальные и духовные ценности) и государство (его конституционный строй, суверенитет, территориальная целостность, экономика, военное дело и т. д.).

Личность – базовый элемент, ячейка общества. Без личности нет общества, но и личность вне общества существовать не может. Государство обеспечивает условия существования и личности, и общества. Государства, которые не нужны ни личности, ни обществу, не могут существовать долго и исчезают с исторической арены. Баланс взаимоотношений между личностью, обществом и государством выступает главным условием их устойчивого развития.

**Информационная безопасность личности** – это состояние человека, в котором его личности не может быть нанесен существенный ущерб путем оказания воздействия на окружающее информационное пространство.

В процессе информатизации человек стал информационно «прозрачен». При наличии желания и средств любая имеющаяся информация о конкретной личности может стать доступной и быть использована в своих целях другой личностью, группой лиц, общественной группой и государством. Только незначительная часть населения способна предотвратить нежелательный доступ к своей информации. Большинство людей такой возможности не имеют и остаются беззащитными в этом плане.

**Информационная безопасность общества** – это состояние общества, в котором ему не может быть нанесен существенный ущерб путем воздействия на его информационную сферу. В ее основе – безопасность индивидуального, группового и массового сознания граждан при наличии информационных угроз, к которым в первую очередь следует отнести информационно-психологическое воздействие. Действие этих угроз может вызывать психоэмоциональную и социально-психологическую напряженность, искажение нравственных критериев и норм, морально-политическую дезориентацию и, как следствие, неадекватное поведение отдельных лиц, групп и масс людей. В результате таких воздействий возможны глубокие трансформации индивидуального, группового и массового сознания, негативные изменения морально-политического и социально-психологического климата в обществе.

**Информационная безопасность государства** – это состояние государства, в котором ему не может быть нанесен существенный ущерб путем оказания воздействия на его информационную сферу. Обеспечение информационной безопасности государства неразрывно связано с обеспечением национальной безопасности.

**2. Информационные войны и информационный терроризм**

Проблемы информационной безопасности государства достаточно полно освещены в Доктрине информационной безопасности Российской Федерации. Остановимся на двух из них: проблеме информационных войн и информационного терроризма.

**Информационная война** – это действия, предпринимаемые для достижения информационного превосходства путем нанесения ущерба информационной сфере противника и обеспечения собственной информационной безопасности.

Информационные войны ведутся с помощью информационного оружия, применение которого по эффективности сравнимо с действием оружия массового поражения. Идея использования и материальные основы современного информационного оружия формировались по мере развития информатизации. Компьютеризация различных сфер общественной жизни, развитие телекоммуникационных и информационных сетей, создание баз и банков данных, широкое внедрение новейших информационных технологий и превращение профессии программиста в престижную и массовую специальность создали базовые научные, технологические и экономические предпосылки для возникновения и совершенствования нового типа информационного оружия и в то же время сделали объекты управления и связи, энергетики и транспорта, банковскую систему весьма уязвимыми по отношению к информационному воздействию.

**Информационное оружие** представляет собой совокупность средств, методов и технологий, обеспечивающих возможность силового воздействия на информационную сферу противника с целью разрушения его информационной инфраструктуры, систем управления государством, снижения обороноспособности.

Универсальность, скрытность, широта воздействий, выбора места и времени применения, эффективность и отсутствие правовых ограничений на использование делают информационное оружие чрезвычайно опасным средством вооруженной борьбы. Оно может применяться и в мирное время. Более того, злонамеренные воздействия на техническую систему, в том числе и военно-техническую, могут быть оказаны уже на этапе ее проектирования и создания за счет преднамеренного внесения специальных дефектов диверсионного типа (программных закладок) в программное обеспечение системы. Сложность современных программных средств практически не позволяет выявить подобные закладки.

Театром военных действий при ведении информационных войн является все мировое информационное пространство, а разрушительная мощь информационного оружия в процессе дальнейшей информатизации будет только усиливаться. Информационные войны, особенно в условиях существования почти монопольного положения в информационной сфере небольшого количества стран, способны вызвать национальные, региональные и даже мировые информационные катастрофы, разрушительные последствия которых для мировой цивилизации будут не менее губительны, чем последствия ядерных катастроф. Угроза информационной войны в глобальном контексте есть фактор скрытого военно-политического давления и запугивания, фактор, способный нарушить стратегический паритет, подорвать сложившееся равновесие на мировой политической арене.

Действия отдельных лиц или групп, направленные на нанесение ущерба информационной сфере или ее использование в корыстных целях, называются **информационным криминалом.** Как правило, это разовые преступления против конкретного объекта информационного пространства.

**Информационный терроризм** – это особая форма насилия, представляющая собой сознательное и целенаправленное информационное воздействие или угрозу применения такого воздействия для принуждения правительства к реализации политических, экономических, религиозных и иных целей террористической организацией или отдельными террористами, сопровождаемое эмоциональным воздействием на общество для возбуждения в нем страха, панических настроений, потери доверия к власти и создания политической нестабильности.

Информационный терроризм при сходстве с информационными войной и криминалом по форме и методам отличается от них целями и тактикой. Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил широкий общественный резонанс. Как правило, требования террористов сопровождаются угрозой повторения террористического акта без указания конкретного объекта действия.

Угроза информационного терроризма стала важным геополитическим фактором, и борьба с ней требует объединения усилий всех государственных институтов, а также активизации международного сотрудничества в этой области.

**3. Угрозы информационной безопасности России**

Следует отметить, что, хотя порождаемые информатизацией проблемы информационной безопасности являются глобальными, для России они приобретают особую значимость в связи с ее геополитическим и экономическим положением.

В Доктрине информационной безопасности Российской Федерации, утвержденной Президентом РФ 9 сентября 2000 г *.,* ***угрозы информационной безопасности*** страны по их общей направленности подразделяются на угрозы:

• конституционным правам и свободам человека и гражданина в области информационной деятельности;

• духовной жизни общества;

**Информационная безопасность**

• информационной инфраструктуре;

• информационным ресурсам.

*Угрозами конституционным правам и свободам человека и гражданина* в области информационной безопасности могут являться:

• принятие органами государственной власти нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области информационной деятельности;

• создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

• противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений, а также неэффективное применение существующей в этой области нормативно-правовой базы;

• нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

• нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

• невыполнение органами государственной власти, организациями и гражданами требований законодательства РФ, регулирующего отношения в информационной сфере.

*Угрозами духовной жизни общества* могут быть:

• применение средств воздействия на массовое сознание граждан;

• дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

• ограничение доступа граждан к открытым государственным информационным ресурсам органов государственной власти, другой социально значимой информации;

• снижение духовного, нравственного и творческого потенциала России;

• манипулирование информацией (дезинформация, сокрытие или искажение информации).

*Угрозами информационной инфраструктуре* могут являться:

• нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

• нарушение технологии обработки информации;

• внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные в документации на эти изделия;

• разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе системы защиты информации;

• уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

• хищение программных или аппаратных ключей и средств криптографической защиты информации;

• перехват информации в технических каналах, ее утечка, возникающая при работе технических средств обработки и хранения, а также во время передачи информации по каналам связи;

• внедрение электронных устройств перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти и организаций;

• уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

• перехват, дешифрование и навязывание ложной информации в сетях передачи данных, линиях связи и системах массовой информации;

• воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

• закупка за рубежом информационных технологий, средств информатизации, телекоммуникации и связи, имеющих отечественные аналоги, не уступающие по своим характеристикам зарубежным образцам.

*Угрозами информационным ресурсам* могут быть:

• деятельность космических, воздушных, морских и наземных технических средств разведки иностранных государств;

• осуществление несанкционированного доступа к информационным ресурсам и их противоправное использование;

• хищение информационных ресурсов из библиотек, архивов, банков и баз данных;

• нарушение законных ограничений на распространение информационных ресурсов.

В своем Послании по национальной безопасности (13 июня 1996 г.) Президент РФ определил ***основные угрозы для России в информационной сфере*** следующим образом:

• *внутренние –* отставание страны от ведущих стран по уровню и темпам информатизации, отсутствие четко сформулированной информационной политики;

• *внешние –* попытки не допустить Россию участвовать на равноправных условиях в международном информационном обмене, вмешательство и целенаправленное проникновение в деятельность и развитие информационной инфраструктуры РФ, стремление сократить использование русского языка как международного средства общения и через это сужение российского информационного пространства.

Эти и другие внутренние и внешние угрозы *по способам воздействия* (реализации) делятся на собственно информационные, программно-математические, физические и организационные.

*Информационные угрозы* реализуются посредством несанкционированного доступа к информационным ресурсам и их хищения в целях противоправного использования, негативного манипулирования информацией (дезинформация, искажение информации, ее сокрытие), нарушения технологии обработки информации и т. д.

*Программно-математические угрозы* реализуются путем внедрения в аппаратные и программные системы компонентов, выполняющих функции, не описанные в документации на эти системы и снижающие эффективность их функционирования, разработки и распространения программ (вирусов, «троянских коней» и др.), нарушающих нормальное функционирование систем, в том числе систем защиты информации.

*Физические угрозы* связаны с физическим воздействием (уничтожение, повреждение, хищение) на информационные системы и их элементы, сигнальным перехватом информации в каналах передачи или в служебных помещениях и т. д.

К *организационным угрозам* следует отнести прежде всего слабую правовую базу обеспечения информационной безопасности. Практически отсутствует правовое обеспечение информационной безопасности на региональном уровне. Требования существующих законодательных актов (Конституция РФ, законы РФ «О безопасности», «О государственной тайне», «Об информации, информатизации и защите информации» и др.) не всегда выполняются. Недостатки правовой системы приводят к тому, что значительный объем информации с ограниченным доступом в финансово-биржевой, налоговой, таможенной, внешнеэкономической, жилищной и других сферах в виде конкретных баз данных распространяется различными коммерческими фирмами.

В *информационном пространстве* с позиции информационной безопасности наиболее типичными *являются две опасности:*

1) *контроль (извлечение) информационных ресурсов государства,* т. е. фактически информационная разведка (шпионаж). Информационное пространство было и остается сферой деятельности многочисленных разведывательных служб. Сегодня информационная разведка может быть реализована двумя путями: несанкционированным проникновением в информационные и управляющие системы; легальным путем, за счет активного участия зарубежных фирм в создании информационной структуры России. При этом кроме негативных последствий, связанных с тем, что информационные ресурсы страны оказываются под контролем соответствующих иностранных структур, наносится прямой урон экономике – остаются без собственных заказов отечественная наука и производство;

*2) угроза разрушения или дезорганизация информационных ресурсов элементов государственных структур.* При современном уровне развития информационных технологий такие воздействия могут осуществляться даже в мирное время. Они чреваты разрушением ценной для государства информации, ее искажением или внедрением негативной информации в целях дезорганизации или принятия неправильных решений на соответствующем уровне государственного управления.

Особое место занимает *безопасность компьютерных сетей,* которые позволяют объединить и совместно использовать большой объем информационных ресурсов локального и глобального масштаба. Компьютерные сети становятся одним из основных средств информационного общения. В то же время их огромные возможности вступают в противоречие с проблемой обеспечения защиты информации. Это обстоятельство необходимо учитывать при создании и развитии как локальных, так и глобальных компьютерных сетей. Так, в процессе создания сети Интернет в США в январе 1981 г. был создан Центр компьютерной безопасности Министерства обороны, в 1985 г. его преобразовали в Национальный центр компьютерной безопасности и передали в Агентство национальной безопасности.

Анализ приведенных угроз, форм и методов их воздействия на объекты безопасности в информационной сфере, а также методов и средств борьбы с этими угрозами позволяет утверждать, что в настоящее время в теории и практике информационной безопасности уже начинают выкристаллизовываться два направления, которые можно определить (хотя и достаточно условно) как информационно-психологическая безопасность и защита информации.

*Информационно-психологическая безопасность –* состояние защищенности граждан, отдельных групп и социальных слоев общества, массовых объединений людей, населения в целом от негативных информационно-психологических воздействий, осуществляемых в информационном пространстве (подробнее об этом речь пойдет далее).

*Защита информации –* обеспечение безопасности информации (парирование угроз информационной инфраструктуре и информационным ресурсам).

В настоящее время наиболее активно разрабатываются проблемы защиты информации: организационные, правовые, технические и технологические меры по предотвращению и отражению угроз информационным ресурсам и системам, устранению их последствий. Формируется теория защиты информации, создаются и активно используются на практике методы и средства защиты информации, осуществляется подготовка специалистов по ряду специальностей и специализаций, таких как технология защиты информации, комплексное обеспечение информационной безопасности автоматизированных систем, безопасность и защита информации и т. д.

**4. Информационная безопасность – важнейший компонент национальной безопасности**

В современном обществе информационная безопасность является системообразующим фактором практически всех сфер его жизни. Она оказывает определенное влияние на состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности. В то же время информационная безопасность сама выступает составной частью национальной безопасности, значение которой с каждым годом неуклонно растет.

Особая роль информационной безопасности объясняется теми глобальными процессами, которые характерны сегодня для социально-экономического развития мира. Поэтому можно уверенно утверждать, что информационная безопасность может рассматриваться как *важнейший компонент национальной безопасности*, «пронизывающий» все остальные виды безопасности. Покажем это на примере социальной и экологической безопасности.

1. *Социальный контекст информационной безопасности.* Проблема социальной (общественной) безопасности была и остается одной из важнейших. Она связана с защитой интересов страны и народа в социальной сфере, развитием социальной структуры и общественных отношений, системы жизнеобеспечения и социализации людей, образа жизни, соответствующего потребностям прогресса нынешних и будущих поколений.

Социальная безопасность имеет многоаспектный характер. В современной России она определяется наличием негативных процессов в обществе, таких как рост преступности, снижение уровня жизни, рост безработицы, разрушение старой системы образования, падение престижа науки и инженерного дела, расслоение общества на богатых и бедных, ухудшение отношений между людьми и т. д.

Гарантом социальной защищенности граждан должны являться конституция, государство, президент и другие институты государственной власти. Главные объекты социальной безопасности – личность и общество, социальные интересы и социальные отношения, а с учетом информационного аспекта – права на получение и использование соответствующей информации, а также система формирования общественного сознания.

С помощью существующих перспективных информационных средств и технологий можно практически полностью контролировать и регулировать информационное взаимодействие людей. Речь идет о потенциальных возможностях подслушивания телефонных (и не только телефонных) разговоров, осуществления контроля за перепиской, создания компьютерных баз данных о каждом человеке, включающих конфиденциальную информацию, и т. д.

Современные информационные технологии позволили резко повысить эффективность средств воздействия на психику людей и общественное сознание, создать новые формы «тихого» («скрытого») манипулирования индивидуальным, групповым и массовым сознанием. Не случайно средства массовой информации называют «четвертой властью». Дальнейшее развитие информационных технологий существенно расширит возможности СМИ, и сила этой власти еще более возрастет. В этой связи вполне обоснованно появление и развитие нового междисциплинарного направления – информационно-психологическая безопасность.

К числу форм «скрытого» воздействия на сознание можно отнести новые технологии средств массовой информации, психотронное оружие, сетевые технологии, позволяющие получать доступ к различной негативной информации, в том числе порнографического, националистического и другого характера, современные компьютерные игры, существенно влияющие на формирование сознания детей, и т. д. (Более подробно вопросы информационной безопасности личности и общественного сознания будут рассмотрены далее.)

2. *Экологические проблемы в структуре информационной безопасности.* Экологическая безопасность – одна из важнейших глобальных проблем современности. Она связана с защитой интересов личности, общества и государства от потенциальных и реальных угроз, создаваемых последствиями антропогенного воздействия на среду, а также от стихийных природных бедствий и катастроф. Рассмотрим информационный аспект этой сложной, многоплановой проблемы.

До сегодняшнего дня сохраняется определенная закрытость процесса формирования экологической политики страны, которая ведется без достаточного информирования научной общественности. В связи с этим не всегда ясно, значится ли экология в числе приоритетов деятельности законодательных и исполнительных органов России или же экологическая проблема используется спекулятивно только в предвыборных баталиях или в борьбе за власть между отдельными группировками. Кроме того, широкие слои населения недостаточно осведомлены об угрозах экологической безопасности, их источниках, о последствиях экологических бедствий и катастроф и т. д. Наиболее характерными примерами этого являются чернобыльская катастрофа, экологические споры, которые велись вокруг строительства скоростной железной дороги Санкт-Петербург – Москва.

Обсуждая экологические проблемы, специалисты часто пользуются *«формулой глобального развития»* Д. Медоуза:

*1=РАТ,*

где *I –* нагрузка на окружающую среду; *Р –* численность населения; Л – уровень благосостояния (потребления на душу населения); *Т –* технология (ущерб среде, наносимый при производстве единицы продукции с использованием определенной технологии).

Данная формула позволяет обнаружить прямую связь между информацией и информационными технологиями и нагрузкой на окружающую среду. Действительно, чтобы уменьшить нагрузки на среду, необходимо совершенствовать производственные процессы, переходить к «экологически чистым», энерго– и ресурсосберегающим безотходным технологиям. А это возможно только при условии коренной перестройки экономики за счет ее информатизации, разработке и широком внедрении новых информационных технологий во все отрасли, в том числе в материальное и энергетическое производство, добывающую промышленность.

В монографии М. Д. Урсула «Путь в ноосферу. Концепция выживания и безопасности развития цивилизации» (М., 1990) и в последующих его работах рассматривается проблема *естественной экологической безопасности,* в основе которой – сохранение биологического разнообразия и устойчивости биосферы. Этот подход выдвигается в качестве альтернативы техногенному (техносферному) пути развития общества. По мнению Урсула, следуя по этому пути, человечество порождает новую угрозу своей безопасности – опасность технократизма. В информационном обществе за счет коренной перестройки экономики благодаря внедрению информационных технологий опасность технократизма значительно уменьшится.

В формуле Д. Медоуза еще одно слагаемое является «информационно управляемым». Речь идет об уровне благосостояния (Л), о формировании разумного стандарта потребления, борьбе с агрессивным потребительским сознанием. Бесспорно, средства массовой информации могут и должны сыграть в этом значительную роль.

Решение большинства экологических проблем и задач связано со сбором и обработкой информации о состоянии природной среды (экологический мониторинг), с моделированием масштабных глобальных процессов, происходящих в природе, с учетом возрастающих техногенных воздействий и антропогенных нагрузок. Очевидно, для эффективного их решения требуется использовать современные информационные средства и технологии.

Таким образом, *проблема национальной безопасности носит ярко выраженный информационный характер.* При этом следует иметь в виду два аспекта:

1. Человек, информационные ресурсы и информационные системы относятся к числу основных элементов объектов безопасности во всех сферах жизнедеятельности государства. Сегодня активно развиваются средства информационного воздействия на них. Поэтому можно утверждать, что проблема информационной безопасности по отношению к другим ее видам носит межвидовой, а по некоторым вопросам надвидовой характер. Этот факт должен учитываться при формировании государственной и региональной политики в области национальной и информационной безопасности, при разработке соответствующих концепций и программ, при организации конкретных работ в области безопасности;

2. Необходимость использования информационного подхода как основного научно-практического метода решения задач национальной безопасности. Эти сложные задачи, связанные со сбором и анализом огромного объема разнородной (по форме представления, по достоверности и т. д.) информации, с моделированием экономических, экологических, социальных, политических, военных, демографических и других процессов в интересах оценки состояния, прогнозирования и принятия решений по важнейшим государственным проблемам, по своей природе являются информационными, для их решения требуется привлекать новые информационные технологии и средства.

**5 Безопасность человека в информационном пространстве**

О серьезности ситуации в сфере воздействия на личность в информационном пространстве свидетельствует широкое использование для описания этого процесса почти военной терминологии: информационная война, информационное оружие, информационная диверсия, информационный терроризм, информационный киллер.

Говоря о безопасности личности в информационном пространстве, кроме понятия «угроза» целесообразно использовать термин «насилие». Как правило, под ним понимается физическое насилие над личностью. В то же время можно и нужно говорить о насилии над личностью в сфере политической жизни, в духовной сфере и т. д. Содержательно угроза – это возможная (потенциальная) опасность, а насилие – фактическая реализация угрозы, принудительное воздействие, в нашем случае информационное, на личность.

Особую актуальность приобретает проблема ***информационно-психологической безопасности,*** что обусловлено многими факторами.

С одной стороны, это *сложные, порой противоречивые и негативные процессы в политической, социально-экономической и духовной сферах,* к которым относятся:

• разрушение старой административно-командной системы и трудное становление новой российской государственности, основанной на демократических принципах;

• трудности перехода к рыночной экономике;

• кризис государственной идеологии;

• деформация системы норм, установок и ценностей;

• рост преступности;

• снижение уровня жизни и рост безработицы;

• расслоение общества на богатых и бедных и ухудшение отношений междулюдьми;

• недооценка национальных и культурно-исторических традиций народов России и проникновение в общественное сознание западной массовой культуры;

• изменение геополитической обстановки;

• деструктивная роль различных форм мифологического сознания и тоталитарных религиозных сект, падение престижа и ослабление важнейших социокультурных институтов государства – науки, образования, воспитания (в том числе физического и психологического) и культуры.

Все это, естественно, может снизить устойчивость личности, ее психики к различным информационным воздействиям. Личность считается устойчивой, если она способна произвести критический анализ, оценку воспринимаемой информации, а также принять объективное решение на основе этой информации.

С другой стороны, это *колоссальный рост эффективности средств информационного воздействия* на психику людей и общественное сознание. Современные и перспективные информационные технологии и средства позволяют управлять информационным взаимодействием людей, общественным сознанием и контролировать их.

В частности, имеются потенциальные возможности подслушивать все телефонные переговоры, осуществлять контроль за перепиской, создавать и противоправно использовать компьютерные базы конфиденциальных данных о персоналиях, осуществлять скрытое информационное воздействие на психику людей и т. д. и т. п.

*Объектами* обеспечения информационно-психологической безопасности являются:

• отдельные граждане, представляющие различные возрастные, социокультурные и национальные группы и слои общества;

• отдельные социальные группы и слои как компоненты социальной структуры общества (в том числе профессиональные, национально-этнические и др.);

• отдельные организации, группы и лица, конкретные представители органов государственной власти и управления, Вооруженных сил, органов правопорядка и безопасности, производственных, финансовых и других структур, осуществляющие деятельность, которая имеет или может иметь важные социальные последствия;

• организованные массовые объединения и самодеятельные группы граждан с собственным особым укладом жизни, системой мотивации, психическим складом, менталитетом и т. п. (Вооруженные силы РФ, беженцы, «афганцы» и др.);

• население конкретных регионов, промышленных и агропромышленных агломераций, отдельных территориальных районов и мест компактного проживания людей и т. д.;

• общественные и политические организации, общественно-политические движения и партии;

• население страны в целом как социально-историческая общность людей, обладающая специфическими особенностями общественной психологии, уникальной системой социокультурных и социопсихологических норм и традиций;

• духовная сфера общества, составляющими которой являются общественное сознание, общественное мнение и социально-психологический климат (в том числе системы образования и воспитания, системы массовой информации, влияющие на социальное поведение и организацию жизнедеятельности людей).

Информационно-психологическая безопасность перечисленных объектов создает условия для обеспечения психического здоровья каждой отдельной личности и населения страны в целом, надежного функционирования государственных и общественных институтов, а также формирования индивидуального, группового и массового сознания с целью прогрессивного развития общества.

*Каналы* (средства) информационного воздействия на личность весьма разнообразны. Это семья, образовательная сфера (детский сад, школа, университет), улица, книги, радио, кино, телевидение, массовая печать (газеты, журналы), аудиовизуальные средства, в частности разнообразная проигрывающая техника (магнитофоны, плееры, видеомагнитофоны), и т. п. На наших глазах рождается новое мощнейшее средство информационного воздействия – Интернет, на очереди техника и технологии виртуальных реальностей, обещающие поистине фантастические перспективы виртуальных воздействий. А визуальная информация наиболее информативна и действенна. Не зря народная пословица гласит: «Лучше один раз увидеть, чем сто раз услышать». Эффективность воздействия этих и других каналов на личность существенным образом повышается за счет активного развития и широкого применения новых информационных технологий.

Информационные технологии – огромное благо для человечества, они определяют будущее общества. Но в то же время в руках злоумышленников это – страшное оружие; главная опасность заключается в несанкционированном доступе (активном или пассивном) к его источнику или потребителю (личности). Последнее и есть информационное воздействие на личность.

Особо следует подчеркнуть *огромные возможности* в этой сфере *современных средств массовой информации.* По существу, сегодня СМИ – практически единственная структура, через которую население ежедневно, ежечасно получает информацию о процессах в стране, регионе, мире. Они буквально навязывают различные идеологические воззрения. Поэтому нельзя не согласиться с мнением, что «сегодня СМИ в России могут выступить и в качестве силы, стабилизирующей обстановку в обществе, и стать детонатором социального взрыва».[62] Особенно актуально это утверждение в период выборных кампаний, которые стали фактически нашей повседневной реальностью. В октябре 1999 г. в Москве даже проводилась научно-практическая конференция «Информационно-психологическая безопасность избирательных кампаний (предотвращение и нейтрализация „грязных“ технологий)».

Как известно, телевидение призвано информировать, просвещать и развлекать. Обращенное непосредственно к человеку и обществу, оно обладает огромной силой информационного воздействия. У нас в стране телевидение с момента своего возникновения выполняет еще и функцию «коллективного агитатора и пропагандиста». В новых социально-экономических условиях эта функция стала реализовываться более откровенно и агрессивно.

В связи с коммерциализацией СМИ, что характерно и естественно для рыночной экономики, с телеэкранов на личность и общество обрушился поток рекламы, фильмы и передачи, пропагандирующие насилие, садизм, секс. Все это можно классифицировать как *несанкционированный доступ к сознанию.* Следствием господства принципа «рекламной паузы» на телевидении является воздействие на психику миллионов людей. Это прямое нарушение прав человека – права на свободный выбор. В идеале реклама должна объявляться в сетке вещания, с тем чтобы каждый имел возможность выбирать ее по собственному желанию.

Непосредственное отношение к безопасности личности в информационном пространстве имеет *проблема обманутых вкладчиков.* В период с 1992 по 1995 г. от действий организаторов финансовых пирамид пострадали около 50 млн россиян. Эти люди, подавляющее большинство которых пожилого возраста, оказались жертвами информационного пресса, той массированной рекламы, которая обещала практически мгновенное сказочное обогащение.

В рыночной экономике информация становится товаром, продуктом, услугой. А это означает, что в целях обеспечения информационной безопасности личности можно использовать законы, защищающие потребителя от недоброкачественной продукции и услуг.

В число ***первоочередных мероприятий, направленных на обеспечение информационной безопасности личности,*** входят следующие.

1. *Развитие информационной культуры* населения, в том числе развитие личностных способов активной и пассивной защиты от опасных информационных воздействий и привитие навыков технологически грамотного продуцирования информации.

2. *Развитие законодательства в информационной сфере.* Основным и, возможно, единственным гарантом соблюдения прав и свобод личности в информационном пространстве является государство. Эту функцию оно может реализовать только через соответствующие законы. Следует отметить, что законодательство в информационной сфере не имеет аналогов в истории. Поэтому к его разработке кроме юристов должны быть привлечены специалисты различных областей, в том числе информатики, информационных технологий, психологии, социологии, педагогики и т. д. В указанном направлении уже сделаны определенные шаги. Рабочей группой Межведомственной комиссии по информационной безопасности под руководством Совета безопасности РФ разработан проект концепции совершенствования правового обеспечения информационной безопасности РФ.

*3. Создание системы мониторинга информационно-технологических факторов риска* (возможно, путем расширения функций структур изучения общественного мнения, обеспеченных соответствующими методиками).

4. *Расширение международного сотрудничества по вопросам безопасности в информационном пространстве.* Диапазон проблем для обсуждения в рамках такого сотрудничества весьма широк. Это и установление согласованной точки зрения по проблемам воздействия информации на индивидуальное и массовое сознание, на психику человека, и подготовка соглашений (конвенций) о неиспользовании информационного пространства во враждебных целях, о контроле над производством и внедрением информационных технологий, которые могут быть использованы в террористических и криминальных целях, о международной правовой защите сетевых информационных ресурсов, о возможности контроля и ограничения распространения по глобальным сетям типа Интернета информации, оказывающей негативное воздействие на физическое, психическое и социальное здоровье людей, особенно детей и молодежи, и т. д.

Без реализации указанных и других мероприятий, направленных на создание необходимых условий для безопасного развития личности в современных условиях, немыслимо и устойчивое развитие экономики, и само будущее развитие России. Безопасность каждого предопределяет безопасность всех, в том числе государства.

**Выводы**

Информатизация общества порождает проблемы информационной безопасности, главные из которых – проблема информационных войн и информационного терроризма. Они носят глобальный характер, но для России приобретают особую остроту, что обусловлено ее геополитическим и экономическим положением.

Угрозы информационной безопасности России подразделяются по общей направленности (угрозы конституционным правам и свободам граждан, духовной жизни общества, информационной структуре, информационным ресурсам) и по способам воздействия (собственно информационные, программно-математические, физические и организационные).

В современном обществе информационная безопасность является важнейшим компонентом национальной безопасности. От нее в значительной степени зависит уровень экономической, оборонной, социальной, политической и других видов безопасности.

В теории и практике информационной безопасности можно выделить два направления: защита информации и информационно-психологическая безопасность. Информационно-психологическая безопасность создает условия для обеспечения психического здоровья отдельной личности и населения страны в целом, надежного функционирования государственных и общественных институтов, а также формирования индивидуального, группового и массового сознания, нацеленного на прогрессивное развитие общества. Информационная безопасность – залог устойчивого развития экономики и общества

**Список литературы:**

1. *Смолян Г.Л.* Сетевые информационные системы и проблемы безопасности личности // Информационное общество. 2001. № 1.
2. *Оценка* эффективности систем защиты информационных ресурсов / Д.С. Черешкин, В.А. Гадасин, О.И. Елизаров и др. М., 2000