

Содержание

Введение.....	2
1. Направления.....	3
1.1. Первое направление.....	3
1.2. Второе направление.....	4
1.3. Третье направление.....	4
2. Правовая защита информации.....	5
3. Информатизация общества и проблема информационной безопасности.....	9
4. Основные цели и объекты информационной безопасности личности.....	11
4.1. Источники угроз информационной безопасности. Основные задачи обеспечения информационной безопасности личности.....	11
Заключение.....	17
Список литературы.....	18

Введение

Особенностью современного периода - является переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергические ресурсы. Ресурсами называют элементы экономического потенциала, которыми располагает общество и которые могут быть использованы для достижения конкретной цели хозяйственной деятельности. Но вот появилось понятие информационные ресурсы, и хотя оно узаконено, то осознано пока ещё недостаточно. Информационные ресурсы - это отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивов, фондах, и т.д.). Информационные ресурсы являются собственностью, подлежат учету и защите, так как информацию можно использовать не только для товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или уничтожить. Собственная информация для производителя представляет значительную ценность, так как нередко получение такой информации - весьма трудоемкий и дорогостоящий процесс. Ценность информации определяется в первую очередь приносимыми доходами.

Целями защиты информации являются: предотвращение разглашения, утечки и несанкционированный доступ к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение

прав субъектов в информационных процессах и при разработки, производстве и применении информационных систем, технологии и средств их обеспечения.

Цель исследования - рассмотреть особенности информационной безопасности личности в современном мире.

Для достижения данной цели необходимо решение следующих задач:

исследовать нормативно-правовые документы по регулированию безопасности личности;

проанализировать информатизацию общества и проблему информационной безопасности;

определить основные цели и объекты информационной безопасности личности, источники угроз информационной безопасности и основные задачи обеспечения информационной безопасности личности.

Объектом исследования является информация в современном мире. Предметом исследования являются методы и средства защиты информации, а так же борьбы с угрозами информационной безопасности.

Методологическую основу исследования составили: методы анализа, синтеза, сравнения, обобщения и др.

Жизненно важные интересы определяются законодателем как совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества, государства, а угроза безопасности - как совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества, государства. И, наконец, обеспечение безопасности - проведение единой государственной политики в этой сфере и система мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление и предупреждение угроз.

1. Направления

1.1.Первое направление

Защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации.

Наиболее острой проблемой современного общества является проблема информационной безопасности, начиная от отдельного человека до государства.



MyShared

1.2. Второе направление

Защита информации и информационных ресурсов, прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц.

1.3. Третье направление.

Защита информационных прав и свобод личности (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; права собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в информационной сфере в условиях информатизации. Рассмотрим их подробнее.

Правовую основу первого направления правового обеспечения информационной безопасности составляют следующие информационно-правовые нормы Конституции РФ.

Законодатель имеет в виду, что свобода массовой информации и запрет цензуры дают возможность создавать и распространять достоверную, своевременную, объективную, т.е. доброкачественную информацию, при которой должно быть исключено распространение вредной и опасной информации. Именно такие требования с точки зрения информационной безопасности должны применяться при формировании института массовой информации, учитываться при подготовке нормативных правовых актов в рамках этого института.

В п. 3 ст. 41 Конституции РФ указано, что сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом.

"Статья 29

Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства".

2. Правовая защита информации

Информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц

Правовую основу второго направления информационной безопасности составляют следующие информационные конституционные нормы.

"Статья 23

Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений..."

При этом прямо запрещается кому бы то ни было собирать информацию о любом гражданине без его на то согласия.

"Статья 24

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются".

Конституцией РФ запрещается также получать иную информацию от любого гражданина без его добровольного на то согласия или убеждать его отказаться от предоставленной ранее информации.

Основной системообразующий набор норм, обеспечивающих защиту информации, информационных ресурсов, информационных систем от неправомерного вмешательства третьих лиц, развивающих содержание конституционных норм, содержится в Федеральном законе "Об информации, информатизации и защите информации".

"Статья 21. Защита информации

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

в отношении персональных данных - федеральным законом".

К конфиденциальной информации относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- сведения, составляющие тайну следствия и судопроизводства;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);

Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством РФ.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством РФ.

Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство РФ.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации".

В целом вопросы этого направления правового обеспечения информационной безопасности условно разделяются на защиту открытой информации и защиту информации ограниченного доступа.

Защита информации ограниченного доступа регулируются нормами: института государственной тайны, института коммерческой тайны, института персональных данных, а также нормами защиты других видов тайн.

Защита информационных прав и свобод обеспечивается нормами институтов интеллектуальной собственности, института документированной информации, УК РФ, КоАП РФ, ГК РФ.

Примеры норм УК РФ: нарушение неприкосновенности частной жизни (ст.137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст.138), отказ в предоставлении гражданину информации (ст.140), нарушение авторских и смежных прав (ст.146), отказ в предоставлении гражданину информации (ст.140), нарушение изобретательских и патентных прав (ст.147), воспрепятствование осуществлению права на свободу совести и вероисповеданий (ст.148), разглашение тайны усыновления (удочерения) (ст.155).

Примеры норм КоАП РФ: воспрепятствование осуществлению гражданином Российской Федерации своих избирательных прав либо работе избирательной комиссии; распространение ложных сведений о кандидате; нарушение прав члена избирательной комиссии (комиссии по проведению референдума), наблюдателя или иностранного (международного) наблюдателя; нарушение права граждан на ознакомление со списком избирателей"; нарушение условий проведения предвыборной агитации через средства массовой информации; изготовление или распространение анонимных агитационных материалов.

Примеры норм ГК РФ: компенсация морального вреда (ст.151), защита чести, достоинства и деловой репутации (ст.152).

Заклячая рассмотрение правовых проблем информационной безопасности, отметим, что информационную безопасность можно рассматривать как аспект или ракурс изучения и формирования системы информационного права, подготовки и совершенствования норм и нормативных правовых актов этой отрасли. Используя результаты исследования в области информационной безопасности, законодатель и исследователь отрасли информационного права получают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Тем самым существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере.

В этой связи структура правового регулирования отношений в области информационной безопасности как бы повторяет структуру самого информационного законодательства, акцентируя внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности. В итоге можно построить некоторую модель основных направлений защиты объектов информационной сферы и институтов информационного законодательства, с помощью нормативных предписаний которых решается проблема правового обеспечения защиты их информационной безопасности. Правовое регулирование информационной

безопасности формируется на базе информационных правоотношений, охватывающих все направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений.

Объекты правоотношений в области информационной безопасности - это духовность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства.

Субъектами правоотношений в области информационной безопасности выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане.

Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений.

Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности. Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.

Ответственность за правонарушения в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной информации и дезинформации; защиты личности в условиях информатизации; защиты информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения.

Правовые основы защиты информации - это законодательный орган защиты информации, в котором можно выделить до 4 уровней правового обеспечения информационной безопасности информации и информационной безопасности предприятия.

Первый уровень правовой охраны информации и защиты состоит из международных договоров о защите информации и государственной тайны, к которым присоединилась и Российская Федерация с целью обеспечения надежной информационной безопасности РФ. Кроме того, существует доктрина

информационной безопасности РФ, поддерживающая правовое обеспечение информационной безопасности нашей страны.

Правовое обеспечение информационной безопасности:

Международные конвенции об охране информационной собственности, промышленной собственности и авторском праве защиты информации в интернете;

Конституция РФ (ст. 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);

Гражданский кодекс РФ (в ст. 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне);

Уголовный кодекс РФ (ст. 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, ст. 273 - за создание, использование и распространение вредоносных программ для ЭВМ, ст. 274 - за нарушение правил эксплуатации ЭВМ, систем и сетей);

Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ (ст. 10 устанавливает разнесение информационных ресурсов по категориям доступа: открытая информация, государственная тайна, конфиденциальная информация, ст. 21 определяет порядок защиты информации);

Федеральный закон «О государственной тайне» от 21.07.93 № 5485-1 (ст. 5 устанавливает перечень сведений, составляющих государственную тайну; ст. 8 - степени секретности сведений и грифы секретности их носителей: «особой важности», «совершенно секретно» и «секретно»; ст. 20 - органы по защите государственной тайны, межведомственную комиссию по защите государственной тайны для координации деятельности этих органов; ст. 28 - порядок сертификации средств защиты информации, от носящейся к государственной тайне); Защита информации курсовая работа.

3. Информатизация общества и проблема информационной безопасности

Информатизация общества - организованный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Деятельность отдельных людей, групп, коллективов и организаций сейчас все в большей степени начинает зависеть от их информированности и способности эффективно использовать имеющуюся информацию. Прежде чем предпринять

какие-то действия, необходимо провести большую работу по сбору и переработке информации, ее осмыслению и анализу. Отыскание рациональных решений в любой сфере требует обработки больших объемов информации, что подчас невозможно без привлечения специальных технических средств.

Возрастание объема информации особенно стало заметно в середине XX в. Лавинообразный поток информации хлынул на человека, не давая ему возможности воспринять эту информацию в полной мере. В ежедневно появляющемся новом потоке информации ориентироваться становилось все труднее. Подчас выгоднее стало создавать новый материальный или интеллектуальный продукт, нежели вести розыск аналога, сделанного ранее. Образование больших потоков информации обуславливается:

чрезвычайно быстрым ростом числа документов, отчетов, диссертаций, докладов и т.п., в которых излагаются результаты научных исследований и опытно-конструкторских работ;

постоянно увеличивающимся числом периодических изданий по разным областям человеческой деятельности;

появлением разнообразных данных (метеорологических, геофизических, медицинских, экономических и др.), записываемых обычно на магнитных лентах и поэтому непопадающих в сферу действия системы коммуникации. Как результат - наступает информационный кризис (взрыв), который имеет следующие проявления :

появляются противоречия между ограниченными возможностями человека по восприятию и переработке информации и существующими мощными потоками и массивами хранящейся информации. Так, например, общая сумма знаний менялась вначале очень медленно, но уже с 1900 г. она удваивалась каждые 50 лет, к 1950 г. удвоение происходило каждые 10 лет, к 1970 г. - уже каждые 5 лет, с 1990 г. - ежегодно;

существует большое количество избыточной информации, которая затрудняет восприятие полезной для потребителя информации;

возникают определенные экономические, политические и другие социальные барьеры, которые препятствуют распространению информации. Например, по причине соблюдения секретности часто необходимой информацией не могут воспользоваться работники разных ведомств.

Эти причины породили весьма парадоксальную ситуацию - в мире накоплен громадный информационный потенциал, но люди не могут им воспользоваться в полном объеме в силу ограниченности своих возможностей. Информационный кризис поставил общество перед необходимостью поиска путей выхода из создавшегося положения.

Информатизация современного общества имеет как положительные, так и отрицательные стороны. Перечислим некоторые опасности и проблемы на пути к информационному обществу:

реальная возможность разрушения информационными технологиями частной жизни людей и организаций;

опасность большого влияния на общество со стороны средств массовой информации;
проблема отбора качественной и достоверной информации при большом ее объеме;
проблема адаптации людей к среде информационного общества, к необходимости постоянно повышать свой профессиональный уровень;
столкновение с виртуальной реальностью, имеющее различные психологические и психические последствия для молодежи;
переход к информационному обществу не сулит каких - либо перемен в социальных благах и усиливает социальную напряженность;
сокращение числа рабочих мест ведет к массовой безработице;
«информационные войны» - открытое или скрытое информационное воздействие государственных систем друг на друга с целью получения определенного выигрыша в политической или материальной сфере. Основными объектами поражения являются информационные инфраструктуры и психология противника.

Развитие глобального процесса информатизации общества, которое наблюдается в последние десятилетия XX века, породило новую глобальную проблему - проблему информационной безопасности человека и общества.

Сущность этой проблемы состоит в следующем. Многие важнейшие интересы личности уже в настоящее время в значительной степени определяются состоянием окружающей их информационной сферы. Поэтому целенаправленные или непреднамеренные воздействия на информационную сферу со стороны внешних или же внутренних источников могут наносить серьезный ущерб этим интересам и представляют собой угрозы для безопасности человека.

В 1998 году начата подготовка и проекта международной концепции информационной безопасности.

Необходимо отметить, что проблемы обеспечения информационной безопасности государства, общества и отдельного человека в значительной степени взаимосвязаны, хотя вполне естественно, что их основные интересы существенно различны. Так, например, на современном этапе развития общества интересы личности заключается в реальном обеспечении своих конституционных прав и свобод, личной безопасности, повышения качества и уровня жизни, возможности физического, интеллектуального и духовного развития.

Интересы общества заключается в достижении и сохранении общественного согласия, повышении созидательной активности населения, духовного развития общества.

Интересы государства состоят в защите конституционного строя, суверенитета и территориальной целостности страны, установлении и сохранении политической и социальной стабильности, обеспечении законности и правопорядка, развитии равноправного международного сотрудничества.

Совокупность перечисленных выше важнейших интересов личности, общества и государства и образует национальные интересы страны, проекция которых на информационную сферу общества и определяет основные цели и задачи страны в области обеспечения информационной безопасности.

4. Основные цели и объекты информационной безопасности личности.

4.1. Источники угроз информационной безопасности. Основные задачи обеспечения информационной безопасности личности.

Во все времена информация играла чрезвычайно важную роль, которая из года в год становилась всё существеннее. В современном обществе она является одним из ключевых экономических ресурсов.

Всем хорошо известно, что «кто владеет информацией, тот владеет миром». Действительно, владение ей в достаточном количестве помогает человеку правильно оценить происходящие вокруг него события, разработать варианты своих действий и принять обдуманное решение. Поскольку информация представляет собой ценность, она может стать объектом купли-продажи, даже кражи (несанкционированного доступа), поэтому она и поддерживающая её инфраструктура должны быть защищены.

Кроме того, информация - сильнейшее средство воздействия на личность, общество и мир в целом. Именно поэтому человечеству в современных условиях требуется механизм фильтрации информации, а впоследствии также инструмент защиты от нежелательной и (или) негативной информации.

Мир стремительно меняется, и, переходя в стадию информационного общества, изменяет все стороны жизни современного человека, независимо от того ребенок это или взрослый. Практически ежесекундно человек подвергается воздействию разнообразной информации, характер которой меняется от полезного и необходимого до откровенно агрессивного. Каждая единица информации, каждое слово, знак, текст несет смысловую нагрузку, воздействующую на ценности человека, его привычки, мотивацию. Устное или печатное слово влияет на психику, зачастую подавляя личность, манипулируя ею. Переход общества на новый информационный уровень развития обуславливает актуализацию проблемы информационной безопасности.

Исходя из всего вышеизложенного, возникает проблема информационной безопасности, и прежде всего именно личности как носителя индивидуальных способностей, характера, интересов.

Вообще, проблема информационной безопасности чрезвычайно многогранна. В ней можно выделить несколько важных аспектов. Во-первых, собственно информационный аспект, связанный с защитой непосредственно информации и информационных ресурсов. К сожалению, большинство существующих

нормативных документов рассматривают информационную безопасность именно в этом контексте, оставляя за гранью, проблемы личности.

Информационная безопасность личности - это:

а) состояние защищённости, при котором отсутствует угроза причинения вреда информации, которой владеет личность;

б) состояние и условие жизнедеятельности личности, при которых отсутствует угроза нанесения вреда личности информацией.

И отсюда следует разделить информационную безопасность на информационно-идеологическую и информационно-техническую. При этом под информационно-технической безопасностью личности следует понимать защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба личности, а под информационно-идеологической безопасностью - защищенность личности от преднамеренного или непреднамеренного информационного воздействия, имеющего результатом нарушение прав и свобод в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащего нравственным и этическим нормам, оказывающих деструктивное воздействие на личность, имеющих негласный характер, внедряющих в общественное сознание антисоциальные установки.

Информационная безопасность личности - это состояние и условие жизни личности, при которой реализуются ее права и свободы.

Жизненно важные интересы - совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К жизненно важным интересам личности относятся: соблюдение и реализацию конституционных прав на поиск, получение, производство и распространение информации; связанные с реализацией права граждан на неприкосновенность частной жизни; использование информации в целях духовного, физического, интеллектуального развития; защиту прав на объекты интеллектуальной собственности; обеспечение прав гражданина на защиту своего здоровья от неосознаваемой человеком вредной информации.

Информационные угрозы	
<i>Преднамеренные</i>	<i>Случайные</i>
1. Хищение информации	1. Ошибки пользователя
2. Компьютерные вирусы	2. Ошибки профессионалов
3. Физическое воздействие на аппаратуру	3. Отказы и сбои, форс- мажор

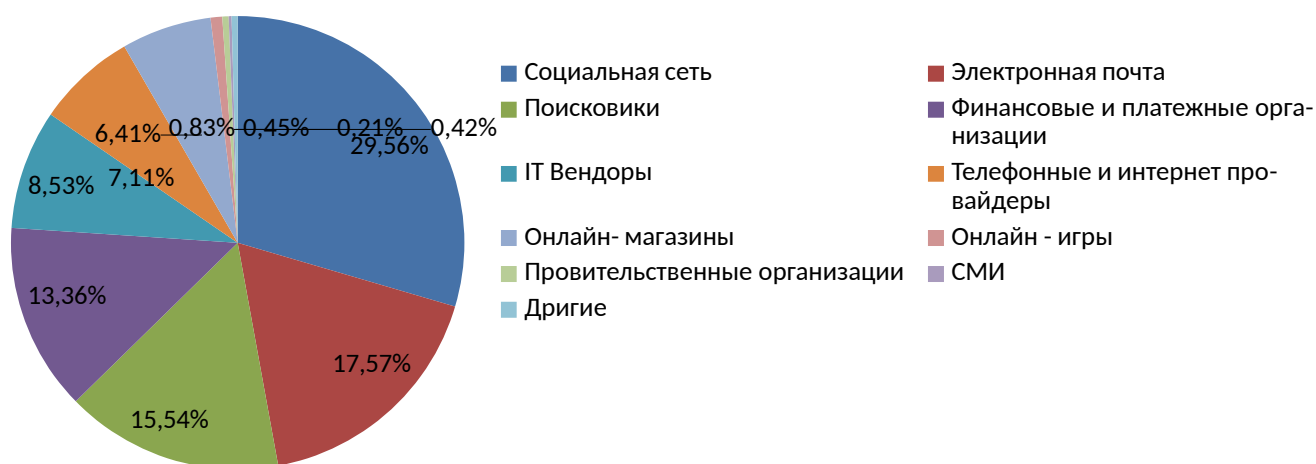
Угроза безопасности - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угрозами информационной безопасности личности являются:

принятие нормативных актов, противоречащих конституционным правам граждан;
 противодействие реализации гражданами прав на неприкосновенность частной жизни;
 неправомерное ограничение доступа к открытой информации;
 нарушение прав граждан в области массовой информации.
 противоправное применение специальных средств, воздействующих на сознание человека;
 манипулирование информацией.

Источниками угроз информационной безопасности личности также могут выступать другая личность, программные и технические средства, группа лиц, общественная группа или даже государство, интернет, СМИ.

Источники угроз в процентах



Доктрина информационной безопасности РФ трактует понятие «информационная

безопасность» как «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Авторы доктрины вполне закономерно связали информационную безопасность личности с ее интересами в области информации, но трактуют данные интересы, по нашему мнению достаточно узко: «Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и

интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность». То есть каждый гражданин должен иметь доступ к легальной информации, может использовать информацию в целях своего всестороннего развития, и защищать информацию, связанную с личной безопасностью гражданина. Таким образом, полностью игнорируется проблема, связанная с разнообразным информационным воздействием на психику человека, и те негативные последствия, которые могут за этим воздействием последовать. В специальной литературе описаны случаи тяжелых форм зависимости связанные с взаимодействием человека глобальными информационными сетями, разнообразные формы игромании, правонарушения, связанные с воздействием информации на личность подростка.

Таким образом, складывается ситуация, когда ни органы власти, ни система образования, ни какие-либо другие социальные институты не в силах контролировать поток информации, обрушивающийся на человека. В этих условиях, проблема информационной безопасности личности человека приобретает ярко выраженный социально-педагогический смысл.

Во-вторых, социально-психологический аспект информационной безопасности, связанный с обеспечением психологической безопасности личности от информационного воздействия.

Анализируя понятие безопасность, С.К.Рощин и В.А.Соснин проанализировали содержание этого понятия на основе определений, даваемых в толковых словарях различных стран. В процессе изучения академических толковых словарей русского, английского, французского и немецкого языков было выявлено, что в народном (общественном) сознании понятие "безопасность" связывается не столько "с отсутствием угрозы", сколько с состоянием, чувствами и переживаниями человека. По мнению авторов, в разных культурах сформировались примерно одинаковые представления о безопасности, акцент в которых делается на чувствах и переживаниях человека, связанных с его положением в настоящем и перспективами на будущее. Иными словами, для человека безопасность переживается в первую очередь как чувство защищенности от действия различного рода опасностей. Исходя из результатов проведенного анализа, авторы сформулировали определение психологической безопасности как состояния общественного сознания, при котором общество в целом и каждая отдельная личность воспринимают существующее качество жизни как адекватное и надежное, поскольку оно создает реальные возможности для удовлетворения естественных и социальных потребностей граждан в настоящем и дает им основания для уверенности в будущем.

Грачев Г.В., в своих исследованиях рассматривает понятие "информационно-психологическая безопасность", которое определяет как состояние защищенности индивидуальной, групповой и общественной психологии и, соответственно, социальных субъектов различных уровней общности, масштаба, системно-структурной и функциональной организации от воздействия информационных факторов, вызывающих социальные процессы. В

социально-психологическом контексте информационная безопасность связывается с разнообразными информационными воздействиями на психику человека, поэтому в данном случае рассматриваются опасности связанные с воздействием на психику отдельного человека, и, соответствующие механизмы защиты от такого воздействия.

Также, можно выделить социологические, социально-политические и другие аспекты данной проблемы. Необходимо определить, что же входит в социально-педагогический контекст понятия «информационная безопасность личности».

Объем и влияние информации, предлагаемой человеку, возросли настолько, что правомерным становится говорить об информационной социализации личности, а сама информация, таким образом, превращается в один из ведущих факторов социализации, такой же мощный как семья, школа или референтная группа. Особенность информации как фактора социализации заключается в том, что он практически неуправляем. Влияние на личность макро - или мезофакторов социализации всегда опосредовано, оно преломляется через деятельность социальных институтов (таких как школа, семья и др.), которые поддаются целенаправленному воздействию, управлению. Информационный поток всегда воздействует непосредственно на личность реципиента. Проведенные опросы показывают, что большинство респондентов характеризуют свою информационную среду как «агрессивную», «недружественную», «вредную». Причем данные характеристики не изменяются у респондентов, принадлежащих к разным социальным слоям и группам. И студенты, и рабочие, и предприниматели, представители интеллигенции проявляют полное единодушие по данному вопросу.

В таких условиях наиболее незащищенными являются дети и подростки, молодежь, еще не выработавшая строгого мировоззрения, четкую жизненную позицию. Поэтому проблема информационной безопасности личности приобретает особую значимость в контексте социально-педагогической деятельности. Так как целью практической социально-педагогической деятельности является гармонизация взаимодействия (отношений) личности и социума для сохранения, восстановления, поддержания, развития социальной активности этого человека. В условиях, когда не учитывается информационный аспект, построить гармоничное взаимодействие личности и социума вряд ли удастся.

По общему мнению, решение проблемы обеспечения информационной безопасности личности, должно носить комплексный системный характер и осуществляться на разных уровнях.

Первый уровень - нормативный. На данном уровне органы государственной власти должны создать непротиворечивую нормативную базу, учитывающую все аспекты проблемы информационной безопасности.

Второй уровень - институциональный, включает в себя согласованную деятельность различных социальных институтов, связанных с воспитанием и социализацией, по обеспечению информационной безопасности личности. В

первую очередь к таким институтам относятся семья, школа для детей и подростков, церковь.

Третий уровень - личностный. Этот уровень связан, прежде всего, с самовоспитанием, самообразованием, формированием высокого уровня информационной культуры личности как части общей культуры человека. На данном уровне происходит формирование необходимых личностных качеств для обеспечения информационной самозащиты личности.

Можно выделить следующие направления профессиональной социально-педагогической деятельности на институциональном и личностном уровнях.

В такой ситуации необходим мощный «щит», который обеспечит информационной безопасностью личность. Такой защитой выступает государство, которое на правовом уровне обеспечивает эту безопасность (Конституция РФ, Доктрина информационной безопасности РФ, законы). Причём надо постоянно совершенствовать законодательную базу, которая должна изменяться «в ногу со временем». Другим средством защиты, на наш взгляд, выступает сама личность, её предусмотрительное отношение к информации, которой она располагает, предоставляет, размещает. Ведь нередко мы сами размещаем информацию о себе (к примеру, в социальных сетях), в беседе расскажем что-то из частной жизни, а потом эта информация, оказавшись в руках заинтересованных лиц, оборачивается против нас. Также информационная безопасность личности обеспечивается на техническом уровне с использованием специальных программ, препятствующих несанкционированному доступу.

Кроме того, необходимо задать определенные нравственные ориентиры, систему ценностей, сформировать национальную идею, иначе информационная защита личности теряет смысл.

В последнее десятилетие происходит активное внедрение компьютерной сети интернет в жизнь общества. Это несёт определённые преимущества, но существует и ряд новых проблем, связанных с появлением интернета, которые пока ни законодательно, ни технически не решены.

Нередко происходит утечка информации из закрытых баз данных, предназначенных для служебного пользования. Проникновение посторонних в эти базы данных происходит через компьютерные сети, в частности, существуют компьютерные вирусы, распространяемые с помощью электронной почты. Впоследствии такая информация может быть беспрепятственно размещена частным лицом в интернете, например, на своём личном сайте. Даже если адрес этого сайта сначала мало кому известен, то существование так называемых поисковых систем - Яндекс, Рамблер, Google и других, делает эту информацию доступной для запроса по каким-либо ключевым словам или фразам документа, по фамилиям людей.

Кроме того, организации могут размещать информацию частного характера о своих сотрудниках на корпоративных сайтах, которые доступны поисковым системам. Так, может быть размещена информация о датах рождения, семейном

положении, номерах домашнего и мобильного телефонов и другая информация, которую работник предоставляет в отдел кадров или другой отдел организации, а не для разглашения в интернете.

С другой стороны, не исключено размещение на каких-либо личных сайтах конфиденциальной информации об организации, её финансовой деятельности, и эта информация также может быть найдена через поисковые системы и нанести ущерб деятельности организации, а для удаления данных необходимо искать авторов сайта, доказать администраторам поисковой системы, что информация конфиденциальная, но и после удаления в течение нескольких недель или месяцев будет доступна «сохранённая копия» документа.

Также не исключается размещение информации личного характера и подробностей личной жизни либо клеветнической информации на личных сайтах или форумах со стороны бывших родственников в случае семейного конфликта и развода. Подобная информация тоже становится доступной поисковым системам. Всё это создаёт угрозу информационной безопасности личности.

Неоднократно имели место случаи утечки информации из баз данных налоговых и финансовых служб. Эта информация продаётся пиратским образом на дисках. Нет гарантии, что подобная закрытая информация, которую человек предоставляет государству, не станет доступна любому пользователю интернета через поисковые системы.

Следует отметить, что в других информационных системах задача об обеспечении информационной безопасности личности ставится и успешно решается. Так, любой абонент может за небольшую сумму немедленно исключить номер своего домашнего телефона из справочной базы данных 09, в справочниках информация о квартирных телефонах в последнее время указывается только с письменного согласия абонента. А справочники по сотовым телефонам отсутствуют и не планируется их издание.

При работе поисковых систем в интернете информационная безопасность личности не только никак не обеспечивается, но даже в ближайшем будущем такая задача не ставится. Требуется разработка нового законодательного подхода к деятельности поисковых систем и новые технические решения.

Таким образом, меры по обеспечению информационной безопасности страны и личности должны быть комплексными и содержать в себе не столько мероприятия идеологического и воспитательного характера, направленные на соответствующую ориентацию общественного сознания.

Заключение

В ходе реализации поставленных задач и достижения цели курсовой работы, сделаны следующие выводы.

Информационная безопасность личности характеризуется степенью ее защищенности и, следовательно, устойчивостью основных сфер

жизнедеятельности личности: экономики, науки, сферы управления, военного дела, общественного сознания.

Правовая наука пока не может остановиться на какой-либо определенной модели в области регулирования и защиты интеллектуальной собственности и особенно исключительных прав создателей информационного и технологического продукта. Тем не менее, закон должен откликаться на коллизии в этой среде. Речь идет о том, что в процессе дополнений и изменений базового Закона и законов субъектов России необходимо уделить большее внимание означенным вопросам. Важное направление работы и области создания адекватной инфраструктуры в сфере информатики формируется вокруг создания и использования таких объектов, как информационные технологии и вычислительная техника.

Информационная безопасность личности определяется способностью нейтрализовать воздействие по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы личности информационным воздействиям на уровне, как внедрения, так и извлечения информации.

Информационная безопасность личности в России является базовой составляющей национальной безопасности России. Она напрямую влияет на эффективную работу органов государственной власти, является неотъемлемым фактором в борьбе с организованной преступностью и мировым терроризмом.

Проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и общества. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

Список литературы

1. Конституция Российской Федерации от 12.12.1993.// Российская газета от 25.12.1993. №237.
2. Гражданский кодекс Российской Федерации (части первая, вторая и третья) // СЗ РФ. 1994. №32. Ст. 33012. Федеральный закон Российской Федерации от 28 декабря 2010 г. N 390-ФЗ «О безопасности»// Российская газета 29 декабря 2010 г. №5374 <<http://www.rg.ru/gazeta/rg/2010/12/29.html>>.
3. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета от 29 июля 2006 г. в № 4131 <<http://www.rg.ru/gazeta/rg/2006/07/29.html>>
4. Федеральный закон от 4 июля 1996 г. N 85-ФЗ "Об участии в международном информационном обмене"//Российская газета. № 129. 11.07.96

5. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. - 208 с.

Алфавитный указатель

	<i>Г</i>		<i>Р</i>	
<i>ГК РФ</i>		<i>18</i>	<i>РФ</i>	<i>18</i>
	<i>К</i>		<i>С</i>	
<i>КоАП РФ</i>		<i>18</i>	<i>СМИ</i>	<i>18</i>

Глоссарии

ГК РФ – Гражданский кодекс Российской Федерации

КоАП РФ - Кодекс об административных правонарушениях Российской Федерации

РФ - Российская Федерация

СМИ - Средство массовой информации (сокращённо «СМИ») — средство донесения информации (словесной, звуковой, визуальной), охватывающее большую аудиторию.