Содержание

Введение

I. Информационная безопасность в Российской Федерации

1.1 Понятие информационной безопасности и ее содержание

1.2 Характеристика угроз информационной безопасности

II. Общая характеристика нормативных правовых актов, регламентирующих обеспечение информационной безопасности

2.1 Общий обзор нормативных правовых актов защиты информации

2.2 Доктрина информационной безопасности Российской Федерации, как основной документ в сфере обеспечения информационной безопасности

Заключение

Список нормативных актов и литературы

Приложение

## Введение

Постановка вопроса в плоскости информационной безопасности имеет особое значение для постсоветской России. В сравнении с прошлым советским периодом развитие Российского государства сориентировано на информационный фактор, без которого невозможна нормальная интеграция в мировое сообщество. Теоретическая и практическая востребованность данной темы диктуется постоянно растущим значением информации и, как следствие, корректного и надежного обеспечения ее доступности лишь определенному кругу лиц, обладающих соответствующей компетенцией.

**Актуальность** данной темы обусловлена следующими обстоятельствами.

Во-первых, качественно новой ролью информации в современном обществе, превращением ее в основной социальный ресурс и параметр цивилизованности современных государств. В настоящее время понятие информации объединяет всю совокупность мировоззренческих и методологических позиций исследователей - от прикладных трактовок ее как сведений, взглядов и знаний, о мире до представлений "первоосновы Вселенной", что обусловлено, главным образом, ее новой ролью в социальной действительности.

Во-вторых, возрастанием политической роли информации, превращением ее в национальный политико-стратегический ресурс и критерий зрелости и развитости политической системы. Сегодня в научном мире информация вполне обоснованно считается политическим капиталом нации. Прогрессивная состоятельность и политический вес страны, ее возможности эффективно влиять на мировые события зависят не только от вещественно-силовых факторов (например, военной и экономической мощи), но и от возможности использовать интеллектуальный потенциал других стран, распространять и внедрять свои духовные ценности, а также тормозить культурную экспансию других народов, трансформировать их культурные ценности.

В-третьих, превращением информационной безопасности в неотъемлемый компонент общей системы безопасности, состояние которой в условиях трансформации российского общества и государства является достаточно проблематичным. Это во многом обусловлено слабостью информационного компонента в переходных условиях развития российского общества и государства, снижением уровня общей безопасности России под воздействием рыночно-демократических факторов "реформирования", ростом так называемой "киберпреступности" и расширением возможностей международного и внутреннего терроризма по использованию современных информационных технологий для подготовки и осуществления террористических актов, особенно на объектах информационной инфраструктуры.

В-четвертых, социальными последствиями низкой отечественной информационной культуры, отставанием информационных технологий России от западных. Как правопреемница бывшего СССР, Россия унаследовала от него достаточно обширную, но не менее отсталую информационную базу. Как известно, доступ к современной информации обеспечивается персональными компьютерами, интегрированными сетями связи и общедоступными базами данных. В СССР этого просто не было, поскольку главным средством доступа к информации и ее переработке являются персональные компьютеры. России еще предстоит создать развитую систему информационного обеспечения, интегрирующую все ее компоненты в интересах безопасного и устойчивого развития.

**Объектом** настоящего исследования являются правоотношения в сфере обеспечения, управления и закрепления мер по осуществлению информационной безопасности в Российской Федерации.

**Предметом** исследования в курсовой работе выступает информационная безопасность Российской Федерации с точки зрения правового закрепления мер, ее обеспечивающих.

Основной **целью** исследования является анализ правовых основ обеспечения информационной безопасности российского общества в условиях глобальной информатизации мирового сообщества, оказывающих на них значительное влияние.

**Степень научной разработанности проблемы.**

В последнее десятилетие информационный компонент общественного развития получил достойное отражение в зарубежной и особенно отечественной литературе. Наиболее приоритетными проблемами, в сфере моего исследования являлись: постановка и разрешение вопроса об информатизации и "информационном обществе" как качественно новом цивилизационном этапе общественного развития[[1]](#footnote-1); раскрытие различных аспектов, проблем, императивов и приоритетов информационной политики государства вообще и российского государства (в виде переложения общих данных на частный случай), в частности[[2]](#footnote-2); раскрытие роли и значения СМИ в условиях современного государства, с учетом стремления Российской Федерации к демократизации правовой базы и приближении ее к стандартам правового государства (что не может не сказаться отрицательно на уровне информационной безопасности в Российской Федерации) [[3]](#footnote-3); обоснование методологических и общетеоретических проблем информационной безопасности[[4]](#footnote-4) и другие проблемы. Теоретико-методологические основы, созданные другими исследователями вопросов информации и информатизации, позволяют успешно исследовать данную проблематику, разрабатывая ее в границах иных информационно-отраслевых направлений.

Данная цель достигается решением следующих задач:

выяснением сущности и содержания информационной безопасности современного российского общества, ее зависимости от политических, технических, социальных и прочих факторов;

исследованием процесса влияния административно-правовых институтов государства современной России на становление и функционирование системы информационной безопасности;

рассмотрением характера дальнейшего развития, приоритетных путей обеспечения и повышения эффективности информационной безопасности российского общества.

**Структура** курсовой работы обусловлена последовательностью реализации исследования рабочей гипотезы и приоритетностью аргументации теоретической проблематики, остротой и актуальностью соответствующей проблематики для современного российского общества и государства, а также степенью разработанности определенных проблем в отечественной и зарубежной литературе.

**Положения, выносимые на защиту:**

1. современному государству, к числу которых Российская Федерация без сомнения относится, просто необходимо создавать систему обеспечения информационной безопасности, опирающуюся на комплекс нормативных правовых актов, которая позволит предупреждать и противодействовать реализации имеющихся угроз информационной безопасности, а также выявлять и принимать меры против уже объективно реализовавшихся угроз

2. В России на данный момент существует и успешно действует целая система обеспечения информационной безопасности, которая, стоит сказать, еще не реализована, то есть не подкреплена гарантиями и не обеспечена правовыми средствами, в полной мере, опирающаяся на Доктрину информационной безопасности Российской Федерации - основополагающий документ, который не только определяет сущность и содержание информационной безопасности такого значимого субъекта международных отношений, как Россия, но и достаточно подробно описывает отдельные ее составляющие, исходя из современных условий социально-политического, экономического и духовно-гуманитарного развития российского государства и может стать моделью для разработки, принятия и практической реализации, аналогичных нормативно-правовых актов в других постсоветских странах.

С учетом отмеченных факторов структура курсовой работы включает введение, две главы, каждая из которых разбита на два пункта, заключение, список нормативных правовых актов и учебной литературы и приложения.

## I. Информационная безопасность в Российской Федерации

## 1.1 Понятие информационной безопасности и ее содержание

Мы считаем, что для полного и правильного понимания правовых основ обеспечения информационной безопасности в Российской Федерации необходимо в первую очередь разобраться в том, какова же сущность и содержание информационной безопасности современного российского общества.

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; даже проводится ФЗ о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности Российской Федерации хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Что же такое "защита информации от несанкционированного доступа" или информационная безопасность Российской Федерации?

Под информационной безопасностью Российской Федерации (информационной системы) подразумевается техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации.

Другими словами вопросы защиты информации и защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Под фразой "угрозы безопасности информационных систем" понимаются реальные или потенциально возможные действия или события, которые способны исказить хранящиеся в информационной системе данные, уничтожить их или использовать в каких-либо целях, не предусмотренных регламентом заранее.

Публикации последних лет свидетельствуют о том, что техника защиты информации, как и правовое регулирование в данном вопросе не успевает развиваться за числом злоупотреблений полномочиями, и всегда отстает в своем развитии от технологий, которыми пользуются взломщики для того, чтобы завладеть чужой тайной.

Существуют документы по защите информации, описывающие циркулирующую в информационной системе и передаваемую по связевым каналам информацию, но документы по защите информации непрерывно дополняются и совершенствуются, хотя и уже после того, как злоумышленники совершают все более технологичные прорывы модели защиты информации, какой бы сложной она не была.

Сегодня для реализации эффективного мероприятия по защите информации требуется не только разработка средства защиты информации в сети и разработка механизмов модели защиты информации, а реализация системного подхода или комплекса защиты информации - это комплекс взаимосвязанных мер, описываемый определением "защита информации". Данный комплекс защиты информации, как правило, использует специальные технические и программные средства для организации мероприятий защиты экономической информации.

Кроме того, модели защиты информации предусматривают ГОСТ "Защита информации", который содержит нормативно-правовые акты и морально-этические меры защиты информации, и противодействие атакам извне. ГОСТ "Защита информации" нормирует определение защиты информации рядом комплексных мер защиты информации, которые проистекают из комплексных действий злоумышленников, пытающихся любыми силами завладеть секретными сведениями. И сегодня можно смело утверждать, что постепенно ГОСТ (защита информации) и определение защиты информации рождают современную технологию защиты информации в сетях компьютерных информационных системах и сетях передачи данных, как диплом "защита информации".

Сегодня существуют следующие виды информационной безопасности, а точнее виды угроз защиты информации на предприятии: пассивная и активная.

Пассивный риск информационной безопасности направлен на внеправовое использование информационных ресурсов и не нацелен на нарушение функционирования информационной системы. К пассивному риску информационной безопасности можно отнести, например, доступ к БД или прослушивание каналов передачи данных.

Активный риск информационной безопасности нацелен на нарушение функционирования действующей информационной системы путем целенаправленной атаки на ее компоненты. К активным видам угрозы компьютерной безопасности относится, например, физический вывод из строя компьютера или нарушение его работоспособности на уровне программного обеспечения. [[5]](#footnote-5)

Защита информации и информационная безопасность строится на следующих принципах:

Построение системы информационной безопасности в России, также как и информационной безопасности организации требует к себе системного подхода, который предполагает оптимальную пропорцию между организационных, программных, правовых и физических свойств информационной безопасности РФ, подтвержденной практикой создания средств защиты информации по методам защиты информации, применимых на любом этапе цикла обработки информации системы.

Непрерывность развития системы управления информационной безопасностью. Для любой концепции информационной безопасности, тем более, если используются методы защиты информации в локальных сетях и компьютерных системах, принцип непрерывного развития является основополагающим, ведь информационная безопасность информации постоянно подвергается все новым и новым с каждым разом еще более изощренным атакам, поэтому обеспечение информационной безопасности организации не может быть разовым актом, и созданная однажды технология защиты информации, будет постоянно совершенствоваться вслед за ростом уровня взломщиков.

Принцип обеспечения надежности системы защиты информации и информационная безопасность - это невозможность снижения уровня надежности системы во время сбоев, отказов, ошибок и взломов.

Обязательно необходимо обеспечить контроль и управление информационной безопасностью, для отслеживания и регулирования механизмов защиты.

Обеспечение средств борьбы с вредоносным ПО. Например, всевозможные программы для защиты информации и система защиты информации от вирусов.

Экономическая целесообразность использования системы защиты информации и государственной тайны. Целесообразность построения системы защиты экономической информации заключается в превышении суммы ущерба при взломе системы защиты информации на предприятии над стоимостью разработки средства защиты компьютерной информации, защиты банковской информации и комплексной защиты информации.

Теперь обратимся к методам и средствам защиты информации, воплощенных в системе организации информационной безопасности, а также о правовом регулировании данного вопроса.

К методам и средствам защиты информации относят организационно-технические и правовые мероприятия информационной защиты и меры защиты информации (правовая защита информации, техническая защита информации, защита экономической информации и т.д.).

*Организационные методы защиты информации и защита информации в России обладают следующими свойствами:*

Методы и средства защиты информации обеспечивают частичное или полное перекрытие каналов утечки согласно стандартам информационной безопасности (хищение и копирование объектов защиты информации);

Система защиты информации - это объединенный целостный орган защиты информации, обеспечивающий многогранную информационную защиту;

*Методы и средства защиты информации и основы информационной безопасности включают в себя:*

Безопасность информационных технологий, основанная на ограничении физического доступа к объектам защиты информации с помощью режимных мер и методов информационной безопасности;

Информационная безопасность организации и управление информационной безопасностью опирается на разграничение доступа к объектам защиты информации - это установка правил разграничения доступа органами защиты информации, шифрование информации для ее хранения и передачи (криптографические методы защиты информации, программные средства защиты информации и защита информации в сетях);

Информационная защита должна обязательно обеспечить регулярное резервное копирование наиболее важных массивов данных и надлежащее их хранение (физическая защита информации);

Органы защиты информации должны обеспечивать профилактику заражение компьютерными вирусами объекта защиты информации.

Очевидно, что эти методы и средства обязательно регламентируются нормами права для создания в государстве, в частности в Российской Федерации, системного и единообразного подхода к их реализации и исполнению.

## 1.2 Характеристика угроз информационной безопасности

При изучении всего комплекса нормативных правовых актов по теме моей курсовой работы мы пришли к выводу, что наиболее полно как сами угрозы, так и их возможные источники перечислены в доктрине информационной безопасности, потому мне показалось целесообразным привести краткий обзор этой части доктрины в этой главы.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Среди вышеперечисленных угроз к сфере внешней информационной безопасности можно отнести следующие.

Из первой группы (угрозы конституционным правам и свободам человека и гражданина): вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур; девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях противоречащих ценностям, принятым в российском обществе; манипулирование информацией (дезинформация, сокрытие или искажение информации), в т. ч. и извне.

Из второй группы (угрозы информационному обеспечению государственной политики РФ): монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами; блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории. [[6]](#footnote-6)

Из третьей группы (угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов): противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий; закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам; вытеснение с рынка российских производителей средств информатизации, телекоммуникации и связи; увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Из четвертой группы (угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России): уничтожение, повреждение, разрушение или хищение машинных и других носителей информации; перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации; использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры; несанкционированный доступ к информации, находящейся в банках и базах данных; нарушение законных ограничений на распространение информации и т.д. [[7]](#footnote-7)

Помимо этого, в доктрине указаны источники угроз информационной безопасности России, среди которых необходимо выделить те из них, которые касаются внешней безопасности.

В соответствии с этим документом источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние, хотя, по мнению автора, между ними существует тесная взаимосвязь. В отдельных случаях внутренние источники могут квалифицироваться как внешние, и наоборот.

К внешним источникам доктрина относит:

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов России в информационной сфере;

стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

обострение международной конкуренции за обладание информационными технологиями и ресурсами;

деятельность международных террористических организаций;

увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам, которые при определенных обстоятельствах могут быть рассмотрены как внешние, относятся: критическое состояние отечественных отраслей промышленности; недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации; недостаточная экономическая мощь государства; недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности; отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти и различных отраслей экономики и социальной сферы и т.д.

При этом необходимо вновь обратить внимание на тесную взаимосвязь между угрозами в сфере внутренней и внешней политики:

К внутриполитическим угрозам, которые непосредственно относятся к сфере международной политики, можно причислить такие как:

Распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

Деятельность общественных объединений, направленная на насильственное изменение конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации. [[8]](#footnote-8)

Примечательно, что в обоих случаях не указывается, идет ли речь о российских или зарубежных структурах, однако очевидно, что такие организации стремятся оказать воздействие на общественное мнение Российской Федерации с целью склонить ее население к тому или иному политическому выбору. По этой причине необходимо еще раз подчеркнуть особую роль средств массовой информации, которые должны учитывать фактор информационной безопасности в своей деятельности. [[9]](#footnote-9)

Внешнеполитическими угрозами, по мнению разработчиков доктрины, для России являются:

Информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

Распространение за рубежом дезинформации о внешней политике РФ;

Нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

Попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях.

Помимо этого, в отдельную группу выделены так называемые внутренние угрозы информационной безопасности России в сфере внешней политики, к числу которых относятся:

Нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

Информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

Недостаточную информированность населения о внешнеполитической деятельности России.

Для решения этих проблем авторы доктрины предлагают:

Разработать основные направления государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;

Разработать и реализовать комплекс мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств России при международных организациях;

Создать российским представительствам и организациям за рубежом условия для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

Совершенствовать информационное обеспечение работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

Совершенствовать информационное обеспечение субъектов РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию. [[10]](#footnote-10)

В этом контексте крайне важным является обеспечить свободный доступ граждан Российской Федерации к любой информации, которая имеет открытый характер и способна содействовать развитию полноценной и гармоничной личности. Это право можно с полной уверенностью оценивать в качестве основополагающего элемента современной концепции прав человека и гражданина. [[11]](#footnote-11)

В сфере науки и техники внешними угрозами являются:

стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничение и т.д.);

политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств - участников СНГ за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

В качестве внутренних угроз в этой сфере безопасности названы такие, как резкое снижение финансирования научных учреждений, утечка за рубеж идей и технологий, технологическое отставание России от западных стран в сфере информационных технологий, что вынуждает российских производителей импортировать зарубежные комплектующие и программное обеспечение, проблемы с патентной защитой российских изобретений и т.д.

Реальный путь противодействия угрозам информационной безопасности РФ в области науки и техники - это, по мнению авторов доктрины, совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации.

В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов РФ по предотвращению противоправного или неэффективного использования интеллектуального потенциала России. [[12]](#footnote-12)

В духовной сфере в качестве угроз определяются: неконтролируемое расширение сектора зарубежных масс-медиа в российском информационном пространстве, использование зарубежными специальными службами средств массовой информации, действующих на территории России, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации, вытеснения русского языка в большинстве постсоветских государств и т.д. [[13]](#footnote-13)

В ответ составители доктрины предлагают заняться духовно-нравственным воспитанием подрастающего поколения и содействовать укреплению патриотизма.

В общегосударственных информационных и телекоммуникационных системах в качестве основной внешней угрозы рассматривается деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля над функционированием информационных и телекоммуникационных систем. Естественной защитной мерой называется усиление защиты информации.

И, наконец, угрозами в сфере обороны для современной России являются:

Все виды разведывательной деятельности зарубежных государств;

Информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

Диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

Деятельность иностранных политических, экономических и военных структур, направленная против интересов РФ в сфере обороны.

Помимо этого, в качестве внутренних угроз для обороноспособности Российской Федерации указаны такие факторы как возможная подрывная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил РФ и их боеготовность, а также нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов.

Для преодоления этих проблемы предлагается систематически выявлять потенциальные угрозы и их источники, структурировать цели обеспечения информационной безопасности в области обороны и определять соответствующие практические задачи; осуществлять защиту информации, которая имеет военное значение, а также более активно применять специфические армейские методы защиты (маскировка, разведка, радиоэлектронная борьба и т.д.). [[14]](#footnote-14)

В целом противодействие информационным угрозам в сфере обороны является одной из наиболее сложных и многофакторных задач по обеспечению национальной безопасности, так как подразумевает целый комплекс психолого-идеологических мероприятий, направленных на сохранение боеспособности вооруженных сил государств и иных силовых структур в мирное и военное время. [[15]](#footnote-15)

Разведывательная деятельность специальных служб иностранных государств, а также международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел рассматривается также в качестве первостепенной угрозы для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах.

Еще одной внешней угрозой является деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов. В данном случае также предлагается обеспечить высочайший уровень защиты конфиденциальной информации и повышать уровень подготовки соответствующих специалистов.

Таким образом, изучив в данной главе квинтэссенцию всего комплекса данных по информационной безопасности, теоретико-методологические основы, заложенные исследователями вопросов информации и информатизации, а также совокупность внешних угроз, представленных в Доктрине информационной безопасности Российской Федерации мы можем позволить себе судить о том, что современному государству, к числу которых Российская Федерация без сомнения относится, просто необходимо создавать систему обеспечения информационной безопасности, опирающуюся на комплекс нормативных правовых актов, которая позволит предупреждать и противодействовать реализации имеющихся угроз информационной безопасности, а также выявлять и принимать меры против уже объективно реализовавшихся угроз

## II. Общая характеристика нормативных правовых актов, регламентирующих обеспечение информационной безопасности

## 2.1 Общий обзор нормативных правовых актов защиты информации

Прежде чем попытаться рассмотреть весь комплекс нормативных правовых актов, регламентирующих сферу обеспечения безопасности в Российской Федерации, стоит сказать, что общее количество законных и подзаконных актов, подходящих под данные требования таково, что окинуть взглядом и рассмотреть их в пределах одной курсовой работы попросту не представляется возможным. Даже поверхностный обзор данных документов займет более чем значительное количество печатных листов. В этом свете вполне понятно желание некоторых авторов каким-либо образом систематизировать и поделить вышеназванные нормативные акты, по каким-либо основаниям, дабы не углубляясь в изучение тонн печатной продукции окинуть взглядом всю правовую систему обеспечения информационной безопасности Российской Федерации. Мне наиболее понятной и целесообразной показалась скомпилированная из нескольких система четырех уровней правовой основы защиты информации, приведенная в учебнике Боера, занимающегося освещением вопросов информационного права, которая приведена далее.

*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 основы защиты информации*

Первый уровень правовой охраны и защиты информации 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 РФ:

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, относящейся к государственной тайне); Защита информации курсовая работа.

Федеральные законы "О лицензировании отдельных видов деятельности" от 08.08.2001 № 128-ФЗ, "О связи" от 16.02.95 № 15-ФЗ, "Об электронной цифровой подписи" от 10.01.02 № 1-ФЗ, "Об авторском праве и смежных правах" от 09.07.93 № 5351-1, "О правовой охране программ для электронных вычислительных машин и баз данных" от 23.09.92 № 3523-1 (ст.4 определяет условие при знания авторского права - знак © с указанием правообладателя и года первого выпуска продукта в свет; ст.18 - защиту прав на программы для ЭВМ и базы данных путем выплаты компенсации в размере от 5000 до 50 000 минимальных размеров оплаты труда при нарушении этих прав с целью извлечения прибыли или путем возмещения причиненных убытков, в сумму которых включаются полученные нарушителем доходы).

Таким образом, правовое обеспечение информационной безопасности весьма на высоком уровне, и многие компании могут рассчитывать на полную экономическую информационную безопасность и правовую охрану информации, и защиту, благодаря ФЗ о защите информации.

*Второй уровень правовой защиты информации*

На втором уровне правовой охраны информации и защиты (ФЗ о защите информации) - это подзаконные акты: указы Президента РФ и постановления Правительства, письма Высшего Арбитражного Суда и постановления пленумов ВС РФ. [[16]](#footnote-16)

*Третий уровень правового обеспечения системы защиты экономической информации*

К данному уровню обеспечения правовой защиты информации относятся ГОСТы безопасности информационных технологий и обеспечения безопасности информационных систем.

Также на третьем уровне безопасности информационных технологий присутствуют руководящие документы, нормы, методы информационной безопасности и классификаторы, разрабатывающиеся государственными органами.

*Четвертый уровень стандарта информационной безопасности*

Четвертый уровень стандарта информационной безопасности защиты конфиденциальной информации образуют локальные нормативные акты, инструкции, положения и методы информационной безопасности и документация по комплексной правовой защите информации рефераты по которым часто пишут студенты, изучающие технологии защиты информации, компьютерную безопасность и правовую защиту информации. [[17]](#footnote-17)

## 2.2 Доктрина информационной безопасности Российской Федерации, как основной документ в сфере обеспечения информационной безопасности

Важнейшим документом в сфере информационной политики, который был принят в России и реализуется в настоящее время, является Доктрина информационной безопасности.

Доктрина информационной безопасности Российской Федерации является базовым концептуальным документом, который определяет основные направления обеспечения одного из ключевых направлений безопасности российского государства. Она была одобрена Советом Безопасности РФ 23 июня и утверждена президентом России В.В. Путиным 9 сентября 2000 г. В доктрине отмечается, что современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Доктрина информационной безопасности служит основой:

для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения

информационной безопасности Российской Федерации;

разработки целевых программ обеспечения информационной

безопасности Российской Федерации.

Как верно отмечает белорусский исследователь С.А. Трахименок, информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности любого государства. [[18]](#footnote-18) Национальная безопасность Российской Федерации также существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать, учитывая, в частности, усиливающиеся угрозы со стороны криминальных группировок, террористов, приверженцев любой экстремальной идеи и других деструктивных общественных сил. [[19]](#footnote-19)

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Решение этой проблемы является первостепенным для дальнейшей разработки доктринальных основ обеспечения информационной безопасности. [[20]](#footnote-20)

В этом документе закреплены четыре составляющие национальных интересов Российской Федерации в информационной сфере. Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина области получения информации и ее использования, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Второй составляющей является информационное обеспечение государственной политики Российской Федерации, которое заключается в доведении до сведения российской и мировой общественности достоверной и позитивной информации о государственной политике России, ее официальной позиции по социально значимым вопросам российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Именно эта составляющая информационной безопасности российского государства имеет самое непосредственное отношение к области внешней политики и отражает важнейшие внешнеполитические задачи Российской Федерации на международной арене.

Для достижения этих целей создатели доктрины предлагают следующие меры:

Укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

Интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третьей составляющей в доктрине названо развитие новых информационно-коммуникационных технологий, в том числе в области индустрии средств информатизации, телекоммуникации и связи, а также обеспечение потребностей внутреннего рынка ее продукцией и выход на мировой рынок.

Эта составляющая национальных интересов Российской Федерации в информационной сфере включает в себя также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого предлагается развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации; развивать индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов; развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем; обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи. [[21]](#footnote-21)

Еще одна составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории РФ. Среди мер, которые предлагается осуществить для реализации этой задачи, называются такие, как повышение безопасности информационных систем, включая сети связи; обеспечение защиты сведений, которые оставляют государственную тайну; расширение международного сотрудничества Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере и т.д.

Особый интерес при анализе текста доктрины представляют виды угрозы информационной безопасности Российской Федерации, которые перечислены в главе первой настоящей курсовой работы.

В доктрине также перечислены меры, которые уже были предприняты федеральными, региональными и местными властями на протяжении 1990-х годов для улучшения ситуации в сфере обеспечения информационной безопасности России. К таким мерам относятся:

Начало формирования базы правового обеспечения информационной безопасности, а именно принятие федеральных законов и работа по созданию механизмов их реализации;

Мероприятия по обеспечению информационной безопасности различных уровней власти,

Укрепление государственной системы защиты информации

Вместе с тем, как утверждается в доктрине, анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства. Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение. Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Недостаточна также государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок. Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Помимо этого, отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В доктрине утверждается, что сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как (нами указаны те, которые касаются сферы обороны, безопасности и внешней политики):

разработка основных направлений государственной политики в области обеспечения информационной безопасности РФ, а также мероприятий и механизмов, связанных с реализацией этой политики;

развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;

разработка федеральных целевых программ обеспечения информационной безопасности РФ;

разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;

развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности применения "информационного оружия";

разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность;

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономическими важными производствами;

развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

создание единой системы подготовки кадров в области информационной безопасности и информационных технологий и т.д.

Исходя из анализа вышеперечисленных пунктов, следует отметить, что на сегодняшний день российское руководство проводит целенаправленную политику по укреплению и расширению информационного обеспечения национальной обороны, безопасности, внешней политики. При этом правительство Российской Федерации не только ставит задачи, но предлагает конкретные методы их решения, которые подразделяются на общие и специальные.

Общие методы, в свою очередь, делятся на правовые, организационно-технические и экономические.

К специальным методам относятся конкретные подходы к обеспечению информационной безопасности в таких сферах как экономика, внутренняя политика, внешняя политика, наука и техника, духовная сфера, общегосударственные информационные и телекоммуникационные системы, оборона, правоохранительная и судебная системы.

Необходимо также отметить, что особое значение в процессе обеспечения информационной безопасности придается международному сотрудничеству в этой сфере. Такое взаимодействие Российской Федерации с другими государствами заявлено как неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Это сотрудничество должно, по мнению разработчиков доктрины, способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Основными направлениями международного сотрудничества Российской Федерации в этой области являются:

запрещение разработки, распространения и применения так называемого "информационного оружия";

обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организационной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При этом авторы доктрины подчеркивают необходимость интенсивного взаимодействия России с другими странами СНГ. [[22]](#footnote-22) Исходя из этого, необходимо еще раз обратить внимание на важность детального анализа отдельных положений доктрины в ходе дальнейшего совершенствования нормативно-правовой базы обеспечения информационной безопасности.

К настоящему времени созданы все условия для обеспечения информационной безопасности Российской Федерации, которое подразумевает всестороннее противодействие имеющимся рискам и угрозам на основании принятой в начале 2000-х годов и действующей в настоящее время политико-правовой основы для этой деятельности.

Таким образом, осуществленный в данной главе анализ нормативных правовых актов, в том числе и Доктрины информационной безопасности Российской Федерации позволяет сделать следующие выводы:

Во-первых, в России на данный момент существует и успешно действует целая система обеспечения информационной безопасности, которая, стоит сказать, еще не реализована, то есть не подкреплена гарантиями и не обеспечена правовыми средствами, в полной мере, опирающаяся на Доктрину информационной безопасности Российской Федерации;

Во-вторых, принятая в 2000 г. доктрина представляет собой основополагающий документ, который не только определяет сущность и содержание информационной безопасности такого значимого субъекта международных отношений, как Россия, но и достаточно подробно описывает отдельные ее составляющие, исходя из современных условий социально-политического, экономического и духовно-гуманитарного развития российского государства.

В-третьих, российская доктрина может стать моделью для разработки, принятия и практической реализации, аналогичных нормативно-правовых актов в других постсоветских странах, особенно учитывая то обстоятельство, что Россия как великая держава сталкивается с несравнимо большим объемом рисков и угроз, чем средние и малые государства.

## Заключение

Подведя итоги нашей курсовой работы можно обобщить все изученное и сделать ряд выводов:

Во-первых, изучая данные по теме нашей курсовой работы мы пришли к выводу, что современному государству, к числу которых Российская Федерация без сомнения относится, просто необходимо создавать систему обеспечения информационной безопасности, опирающуюся на комплекс нормативных правовых актов, которая позволит предупреждать и противодействовать реализации имеющихся угроз информационной безопасности, а также выявлять и принимать меры против уже объективно реализовавшихся угроз;

Во-вторых, в России на данный момент существует и успешно действует целая система обеспечения информационной безопасности, которая опирается на Доктрину информационной безопасности Российской Федерации - основополагающий документ, который не только определяет сущность и содержание информационной безопасности такого значимого субъекта международных отношений, как Россия, но и достаточно подробно описывает отдельные ее составляющие и может стать моделью для разработки, принятия и практической реализации, аналогичных нормативно-правовых актов в других странах.

Также можно сделать заключение, что именно это направление государственной политики России является на сегодняшний момент одним из приоритетных элементов внешнеполитической стратегии российского государства. Поскольку эффективность информационной безопасности в значительной степени определяет место и роль любого государства в мировой политике, то правительство России начало уделять особое внимание реализации этой задачи в первой половине 2000-х годов. В этот период российская внешняя политика претерпела наиболее значимые изменения, вызванные постепенным преобразованием постсоветского пространства под усиливающимся контролем других влиятельных субъектов международных отношений.

В этих условиях Российская Федерация предприняла ряд усилий, направленных на укрепление присутствия в мировом информационном пространстве, которые свидетельствуют о том, что государственная информационная политика России нацелена в настоящее время на формирование и поддержание благоприятного имиджа российского государства. С этой целью используется деятельность структур внешнеполитического и внешнеэкономического аппарата (дипломатических и консульских представительств, информационных центров, торговых домов и т.д.), которые не только выполняют свои прямые обязанности, но и обязаны пропагандировать российские традиции и культурные ценности.

При этом следует подчеркнуть, что на сегодняшний день осуществление этих задач наталкивается на целый ряд проблем, связанных, в первую очередь, с недостатком финансирования государственной информационной политики Российской Федерации за рубежом. Еще одной проблемой является недостаток профессиональных специалистов, которые способны эффективно решать информационные задачи за пределами России. И, наконец, еще одной составляющей указанного комплекса проблем является слабая теоретическая разработка основ современной российской политики в указанной сфере, о чем, к примеру, свидетельствует незначительное количество публикаций по избранной теме.

Необходимо также отметить, что в ближайшем будущем межгосударственная кооперация Российской Федерации в области обеспечения информационной безопасности потребует тесного взаимодействия, учитывая стремление третьих стран оказать влияние на информационное пространство России.

## Список нормативных актов и литературы

1. Нормативные правовые акты:

1. Конституция Российской Федерации, принята в 1993 году на всенародном голосовании;

2. Федеральный закон "Об информации, информатизации и защите информации" от 20.02.95 № 24-ФЗ;

3. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: "Дашков и К", 2003;

4. Федеральный закон "О государственной тайне" от 21.07.93 № 5485-1;

5. Федеральный закон "О лицензировании отдельных видов деятельности" от 08.08.2001 № 128-ФЗ;

6. Федеральный закон "О связи" от 16.02.95 № 15-ФЗ;

7. Федеральный закон "Об электронной цифровой подписи" от 10.01.02 № 1-ФЗ;

8. Федеральный закон "Об авторском праве и смежных правах" от 09.07.93 № 5351-1;

9. Федеральный закон "О право вой охране программ для электронных вычислительных машин и баз данных" от 23.09.92 № 3523-1;

10. О государственной политике в области телевещания и радиовещания: Постановление Государственной Думы от 24 нояб. 2000г. // Законодательство России. - Электронная библиотека Ваше право. - 2003;

2. Учебная и научная литература:

1. Абдеев Р.Ф. Философия информационной цивилизации. - М, 1994;

2. Арский В.Г., Гиляровский И.А., Гуров А.Н., Чёрный И.А. Инфосреда: информационные структуры, системы и процессы в науке и обществе. - М., 1996;

3. Буданцев Ю.П. Системность в изучении массовых информационных процессов. - М., 1986;

4. Виноградова С. .М. Международный обмен информацией: проблемы свободы и ответственности // Информационное общество. Некоторые аспекты. - СПб, 1999;

5. Конецкая В.П. Социология коммуникации. - М., 1998;

6. Копылов В.А. Информация как объект правового регулирования // НТИ. Сер.1. - 1996. - №8; Мелюхин И. Проблемы формирования основ информационного общества в России // Информационные ресурсы России. - 1997. - №6;

7. Моисеев Н.Н. Информационное общество как этап новейшей истории // Свободная мысль, 1996. - №1;

8. Панарин А.С. Глобальное информационное общество: вызовы и ответы // Власть, 2001. - №1;

9. Пирогов А.И. Информатизация российского общества и укрепление обороноспособности страны. - Дисс. … д-ра филос. наук. - М.: ВУ, 1996;

10. Почепцов Г.Г. Теория и практика коммуникации. - М., 1998;

11. Ракитов А.И. Компьютерная революция и информатизация общества. - М., 1990;

12. Суханов А.П. Информация и прогресс. - Новосибирск, 1981;

13. Тихомиров М.Ю. Информационное общество: философские проблемы управления наукой и образованием. - М., 1999;

14. Урсул А.Д. Информация: методологические аспекты. - М., 1974;

15. Уэбстер Ф. Теории информационного общества / Пер. с англ. М.В. Арапова, Н.В. Малыхиной. Под ред. Е.Л. Вартановой. - М.: Аспект Пресс, 2004 и др.;

16. Боер В.М. Информационно-правовая политика государства. - СПб.: СПб. ГУ, 1998;

17. Гаджиев К.С. Средства массовой информации и политика // Вестник МГУ. - Сер.18. - 1995. - №1;

18. Кирюшин С.Ю. К вопросу о роли СМИ в политике // Права человека и гражданина: законодательство и практика. Материалы международной научной конференции.17 марта 2001г.

19. Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. - М.: Горячая линия - Телеком, 2003;

20. Нисневич Ю.А. Информационный фактор политической модернизации // Вестник МГУ. - Сер.12. - 2001

21. Судоргин О.А. Императивы и приоритеты политики обеспечения информационной безопасности России. - Дисс. … канд. полит. наук. - М.: МГОУ, 2005;

22. Андреев Э.М. Средства массовой информации в реформировании России // Социально-политический журнал. - 1996. - №4;

23. Давыдов Л. В.: Роль средств массовой информации в обществе // Вестник МГУ. - Сер.10. - 1995. - №2; Средства массовой информации постсоветской России. - М, 2002;

24. Бусленко Н.И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ. - Дисс. … д-ра полит. наук. - Ростов на Дону, 2003;

25. Информационная безопасность российского государства: социально-политические и социокультурные проблемы. - М., 2001;

26. Ильюшенко В.Н. Информационная безопасность общества. Учебное пособие. - Томск, 1998;

27. Кулаков В.Г. Региональная система информационной безопасности: угрозы, управление, обеспечение. - Автореф. дисс. … д-ра техн. наук. - Воронеж, 2005;

28. Трахименок С.А. Безопасность государства. Методолого-правовые аспекты. Мн.: "Хата", 1997;

29. Уткин А.И. Глобализация: процесс осмысления. М.: "Логос", 2001;

30. Турарбекова Р.М. Информационное неравенство на Ближнем и Среднем Востоке: мифы и реальность // Белорусский журнал международного права и международных отношений. 2002. № 2. http://beljournal. by.ru/2002/2/index. shtml.21.04.2006;

31. Информационное право. Уч пос Ч.1\_Боер В.М., Павельева О. Г\_\_ГУАП, 2006;

32. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Под общ. Ред.А.Е. Тараса. Мн.: Харвест, 1999.;

33. Алпатов В. М.150 языков и политика 1917-2000. Социолингвистические проблемы СССР и постсоветского пространства. М.: "Крафт+", Институт востоковедения РАН, 2000;

34. Права человека. Учеб. Пособие / Авт.-сост. С.П. Кацубо, И.В. Кучвальская, С.Б. Лугвин. Мн.: Амалфея, 2001. Выборы: правовые основы, избирательные технологии. Научн. правовое и практ. пособие / Отв. ред. С.А. Альфер; науч. ред. М.Ф. Чудаков. Мн.: Тесей, 2000.

## Приложение

**Опрос: правовая информированность** Респондентам была предложена анонимная анкета, состоящая из 16 вопросов.

Анализ полученных данных позволил сделать следующие вы воды:

1. Подавляющее большинство респондентов считают себя людьми знающими, что такое право (75%), но лишь половина из них интересуется данным общественным явлением (47%).

2. Действующая в настоящее время правовая система не удовлетворяет правовым потребностям и представлениям 71% опрошенных, но при этом только 13% готово к активной работе по изменению существующей ситуации.

3. В основном, в случае нарушения своего права, молодые люди предпочитают обращаться в специальные правоохранительные органы (60,5%), но при этом только половина из них доверяет им (34%).

4. Уровень правовой информированности респондентов - средний:

59,5% - знакомы с содержанием Конституции Российской Федерации;

64% - знают основные законы, регулирующие их жизнь;

но лишь 42% - знают, кто принимает в Российской Федерации законы.

При этом необходимо заметить, что респондентам был прочитан курс лекций по дисциплине "Основы права". Примечательно, что большинство правильных ответов было получено от курсантов. Не подтверждает ли это необходимость более требовательного, основательного подхода к обучению, которого, безусловно, придерживается военнообразовательная система.

5. Основным источником получения информации остаются СМИ (72%).

6. Уровень общей культуры респондентов, на сугубо субъективный взгляд авторов, ниже среднего. При этом большинство (46,5%) предпочитает отечественные фильмы зарубежным, что, хотя и не говорит об уровне общей культуры, но косвенно указывает на патриотизм и гуманизм молодежи. При появлении свободных денег 26,5% предпочитают потратить их на книги, 20% - на посещение театра, однако 43,5% все же предпочли дискотеку. Большая часть респондентов считают себя завсегдатаями библиотек города (64%), что, впрочем, объясняется необходимостью учебы.

По мнению В.П. Сальникова, с которым трудно не согласиться, правовая информированность способствует добросовестному осуществлению юридических обязанностей, воплощению законодательных актов в практические дела и поступки людей, полному использованию демократических прав и свобод, по существу выступает действенным инструментом реализации творческой роли права. Кроме того, она дает возможность компетентно судить обо всех процессах и явлениях правовой жизни, воспитывает уважение к правовому закону, развивает творческое мышление, содействует утверждению средствами права социальной справедливости, искоренению бюрократизма, попыток некоторых граждан нарушать закон, а также формирует правовую культуру и обеспечивает гражданскую активность личности.1

Без глубоких правовых знаний, безусловно, невозможна точная и обоснованная оценка правовых явлений, формирование установок личности. Таким образом, правовые знания являются первичной ступенью в формировании правовой культуры, а сама правовая культура - это осознание ценности и позитивное отношение к праву, выражающееся в определенной мировоззренческой позиции личности к действующему праву и правомерному поведению.

1. 1 Абдеев Р.Ф. Философия информационной цивилизации.- М, 1994; Арский В.Г., Гиляровский И.А., Гуров А.Н., Чёрный И.А. Инфосреда: информационные структуры, системы и процессы в науке и обществе.- М., 1996; Буданцев Ю.П. Системность в изучении массовых информационных процессов.- М., 1986; Виноградова С..М. Международный обмен информацией: проблемы свободы и ответственности // Информационное общество. Некоторые аспекты.- СПб, 1999; Конецкая В.П. Социология коммуникации.- М., 1998; Копылов В.А. Информация как объект правового регулирования // НТИ. Сер.1. – 1996. - №8; Мелюхин И. Проблемы формирования основ информационного общества в России // Информационные ресурсы России. – 1997. - №6; Его же: Проблемы становления информационного общества // Информационные ресурсы России. – 1997. - №5; Моисеев Н.Н. Информационное общество как этап новейшей истории // Свободная мысль, 1996. - №1; Панарин А.С. Глобальное информационное общество: вызовы и ответы // Власть, 2001. - №1; Пирогов А.И. Информатизация российского общества и укрепление обороноспособности страны. – Дисс. … д-ра филос. наук. – М.: ВУ, 1996; Почепцов Г.Г. Теория и практика коммуникации.- М., 1998; Ракитов А.И. Компьютерная революция и информатизация общества. – М., 1990; Суханов А.П. Информация и прогресс.- Новосибирск, 1981; Тихомиров М.Ю. Информационное общество: философские проблемы управления наукой и образованием. – М., 1999; Урсул А.Д. Информация: методологические аспекты.- М., 1974; Уэбстер Ф. Теории информационного общества / Пер. с англ. М.В.Арапова, Н.В.Малыхиной. Под ред. Е.Л.Вартановой. – М.: Аспект Пресс, 2004 и др. [↑](#footnote-ref-1)
2. Боер В.М. Информационно-правовая политика государства. – СПб.: СПб.ГУ, 1998; Гаджиев К.С. Средства массовой информации и политика // Вестник МГУ. – Сер.18. – 1995. – №1; Кирюшин С.Ю. К вопросу о роли СМИ в политике // Права человека и гражданина: законодательство и практика. Материалы международной научной конференции. 17 марта 2001г.– Краснодар: КГУ, 2001; Манойло А.В., Петренко Л.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Горячая линия – Телеком, 2003; Нисневич Ю.А. Информационный фактор политической модернизации // Вестник МГУ. – Сер.12. – 2001; О государственной политике в области телевещания и радиовещания: Постановление Государственной Думы от 24 нояб. 2000г. // Законодательство России. – Электронная библиотека Ваше право. – 2003; Судоргин О.А. Императивы и приоритеты политики обеспечения информационной безопасности России. – Дисс. … канд. полит. наук. – М.: МГОУ, 2005; [↑](#footnote-ref-2)
3. Андреев Э.М. Средства массовой информации в реформировании России // Социально-политический журнал.- 1996.- №4; Давыдов Л.В. : Роль средств массовой информации в обществе // Вестник МГУ.- Сер.10.- 1995.-№2; Средства массовой информации постсоветской России.- М, 2002; [↑](#footnote-ref-3)
4. Бусленко Н.И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ. – Дисс. … д-ра полит. наук. – Ростов на Дону, 2003; Информационная безопасность российского государства: социально-политические и социокультурные проблемы. – М., 2001; Ильюшенко В.Н. Информационная безопасность общества. Учебное пособие. – Томск, 1998; Кулаков В.Г. Региональная система информационной безопасности: угрозы, управление, обеспечение. – Автореф. дисс. … д-ра техн. наук. – Воронеж, 2005; [↑](#footnote-ref-4)
5. Бачило И.Л. Информационное право: основы практической информатики. Учебное пособие. М.: 2001. [↑](#footnote-ref-5)
6. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-6)
7. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-7)
8. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-8)
9. Выборы: правовые основы, избирательные технологии. Научн. правовое и практ. пособие / Отв. ред. С.А. Альфер; Науч. ред. М.Ф, Чудаков. Мн.: Тесей, 2000. [↑](#footnote-ref-9)
10. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-10)
11. Права человека. Учеб. Пособие / Авт.-сост. С.П. Кацубо, И.В. Кучвальская, С.Б. Лугвин. Мн.: Амалфея, 2001. [↑](#footnote-ref-11)
12. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-12)
13. Алпатов В.М. 150 языков и политика 1917-2000. Социолингвистические проблемы СССР и постсоветского пространства. М.: «Крафт+», Институт востоковедения РАН, 2000. [↑](#footnote-ref-13)
14. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-14)
15. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Под общ. Ред. А.Е. Тараса. Мн.: Харвест, 1999. [↑](#footnote-ref-15)
16. Напр. Доктрина информационной безопасности за № Пр1895 от 9 сентября 2000 г. [↑](#footnote-ref-16)
17. Информационное право. Уч. пос. Ч.1\_Боер В.М., Павельева О.Г\_\_ГУАП, 2006 [↑](#footnote-ref-17)
18. Трахименок С.А. Безопасность государства. Методолого-правовые аспекты. Мн.: «Хата», 1997. [↑](#footnote-ref-18)
19. Уткин А.И. Глобализация: процесс осмысления. М.: «Логос», 2001. [↑](#footnote-ref-19)
20. Турарбекова Р.М. Информационное неравенство на Ближнем и Среднем Востоке: мифы и реальность // Белорусский журнал международного права и международных отношений. 2002. № 2. http://beljournal.by.ru/2002/2/index.shtml. 21.04.2006. [↑](#footnote-ref-20)
21. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-21)
22. Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. [↑](#footnote-ref-22)