САНКТ-ПЕТЕРБУРГСКИЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ

ПРОФСОЮЗОВ

Красноярский филиал

Специальность 021100 "юриспруденция"

Дисциплина: Безопасность предпринимательства и личности

Контрольная работа

Тема: Информационно-коммерческая безопасность предпринимательской деятельности

Выполнил: студент 5-ЮСО

Проверил: к. ю. н., Тепляшин П.В.

Красноярск 2008

**ПЛАН**

|  |  |
| --- | --- |
|  | Введение |
| 1.  | Информационные ресурсы |
| 2.  | Информация как объект правовой защиты  |
| 3.  | Классификация информации по категориям доступа |
| 4.  | Конфиденциальность информации |
| 5.  | Государственная тайна |
| 6.  | Коммерческая тайна |
| 7.  | Защита информации |
| 8.  | Угрозы конфиденциальности информации |
| 9.  | Меры по защите информации |
|  | Заключение  |
|  | Список использованной литературы |

# Введение

Возрастание роли информации практически во всех областях жизнедеятельности обусловлено многими факторами и, прежде всего, формированием информационного сектора экономики, равного по значимости, а порой и превосходящего по ресурсному потенциалу такие традиционные ее подразделения, как промышленность, сельское хозяйство и услуги.

Мера развитости информационного сектора не только оказывает существенное влияние на систему производственных отношений, но и предопределяет реальные границы возможностей для членов общества искать, получать и распространять информацию. Благодаря этому закладывается основа существования системы информационных отношений в обществе, намечаются ориентиры государственной политики в информационной сфере, а информационные процессы нашего общества становятся предметом сознательной, целенаправленной и научно обоснованной деятельности.

Важную роль в проектировании информационных процессов играет право, с помощью которого не только регулируются сложившиеся отношения, но и происходит расширение сферы информационной деятельности, диктуемое общественными потребностями. Таким образом, право воздействует непосредственным образом на ход информационных процессов, определяя и поддерживая те направления, которые формируют облик так называемого информационного общества. Информационное общество развивается стремительными темпами, и это развитие сказывается на характере общественных отношений, складывающихся между членами данного общества, а также между ними и государством. Сущность и характер этих общественных отношений не позволяют осуществить их регулирование нормами только классических отраслей права, поскольку они специфичны в силу особенностей и юридических свойств информации, выступающей в роли основного объекта, по поводу которого и возникают такие отношения.

Обычно предмет права есть вещь материального мира, имеющая определенные физические характеристики. Такими характеристиками может обладать носитель информации, но не сама информация. В Федеральном законе "Об информации, информатизации и защите информации" под информацией понимаются в том числе не материализованные сведения о лицах, предметах, фактах, событиях, явлениях и процессах, отраженные в образах, в том числе и вербальных. Коммерческая информация должна расцениваться как объект правоотношений, реализующийся и существующий в форме общественного отношения по его защите или использованию. Коммерческая (в том числе банковская) тайна связана с интересами обеспечения законной предпринимательской деятельности[[1]](#footnote-1).

## 1. Информационные ресурсы

Изменение человеком окружающего мира влечет развитие информационного пространства. На каждом этапе этого развития неизбежно накапливается информация первого порядка - опыт деятельности человека и информация второго порядка - сведения об опыте обработки и переработки информации. Накапливающийся опыт деятельности человека, фиксируется в виде информации - это служит основной предпосылкой возникновения информационной деятельности и информационных технологий.

Итак, информация – это сведения, независимо от формы их представления, усваиваемые субъектом в форме знаний.

Информационная система – это организационно упорядоченная совокупность документов (информационных продуктов) и информационной инфраструктуры. Примеры информационных систем - библиотеки, архивы, фильмотеки, базы данных, Internet.

Информационные ресурсы - это отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах. [[2]](#footnote-2)

Некоторые авторы предлагают более широкое определение информационного ресурса. Информационный ресурс - это информация, созданная и/или обнаруженная, зарегистрированная, оцененная, с определенными (заданными) законами деградации и обновления. В конце концов, это тоже документ, но с четко определенными качественными и количественными характеристиками. Таким образом, информация, став информационным ресурсом, приобретает присущие только этому понятию (величине) свойства, сохраняя свои собственные. [[3]](#footnote-3)

Мировые и национальные информационные ресурсы можно разделить на:

- Традиционные информационные ресурсы

- Электронные информационные ресурсы

- Формальная и неформальная коммуникация информации

## 2. Информация как объект правовой защиты

Информация как предмет отношений различных субъектов является объектом внимания отраслей и публичного, и частного права. Многие вопросы информации, информационных ресурсов являются объектом норм международного права.

Что касается информационных ресурсов как предмета правовых отношений, то здесь на первом месте находится такой институт права, как правовой режим.

Триединство информации, технологий и систем связи определяет значение института правового режима не только для информационного ресурса. Этот институт действует и в отношениях, связанных с информационными технологиями, образуемыми на их основе информационными системами и обеспечивающими взаимодействие систем средств связи.

С введением в 1996 году нового Гражданского кодекса впервые в российском законодательстве информация стала полноправным объектом права, что закреплено в статье 128 "Виды объектов гражданских прав", которая гласит: "К объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность) нематериальные блага"[[4]](#footnote-4).

Само определение информации вызывает сегодня большие споры. Как отмечалось выше, у разных авторов мы можем найти различные толкования этого термина. Вероятно, было бы ошибкой отдавать приоритет лишь какому-то одному из них.

Российское законодательство определяет информацию как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; документированную информацию (документ) - как зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать[[5]](#footnote-5).

Несмотря на кажущуюся простоту данных определений, уяснение фактической сущности понятия "информация" - дело непростое, так как данное понятие весьма широко и не всегда удачно используется и в законодательстве, и в литературе, и в обиходной речи.

Анализ действующего законодательства позволяет сделать вывод: любая информация в момент своего создания является тайной или конфиденциальной и подлежит дальнейшей защите ее собственником в зависимости от степени секретности. Так, в ст.2 Федерального закона Российской Федерации "Об информации... " устанавливается, что конфиденциальной информацией является документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, а ст.21 устанавливает правило, согласно которому "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:

* сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
* конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего федерального закона;
* персональных данных - федеральными законами.

Как может и должна осуществляться правовая защита информации как одного из объектов собственности? Специфика информации как объекта собственности заключается в том, что правовое регулирование информации должно исходить из возможности защиты информации как по форме выражения, так и по существу содержания одновременно, что требует рассмотрения информации как самостоятельного вида объектов собственности.

## 3. Классификация информации по категориям доступа

Тайны имеют градацию по степени секретности. Так, Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" устанавливает три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности: "Особой важности", "Совершенно секретно" и "Секретно" (ст.8 указанного закона). Собственником информации могут использоваться также грифы "Конфиденциально" и "Для служебного пользования".

Вопросы конфиденциальности всегда тесно связаны с вопросами собственности на информацию, поскольку именно собственник обычно является жертвой при совершении информационных преступлений.

Известно, что в Российской Федерации существует право собственности граждан, юридических лиц и государства (ст.212 ГК РФ). Это законодательное установление позволяет в дальнейшем определить режим использования различных видов информации. Поэтому собственниками информации являются граждане, юридические лица и государство.

Законодательно установлена защита нескольких видов информации, принадлежащей гражданам и называемой "личной конфиденциальной информацией" или "персональными данными".

Коммуникационные тайны: тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч.2 ст.23 Конституции РФ; ст.138 УК РФ); тайна усыновления (ст.155 УК РФ; ст.39 Семейного кодекса РФ); сведения о частной жизни лица (ст.137 УК РФ; ст.150 ГК РФ); личная тайна (ст.137 УК РФ, ст.150 ГК РФ); семейная тайна (ст.137 УК РФ, ст.150 ГК РФ), тайна голосования (ст.142 УК РФ), информация, являющаяся объектом авторских и смежных прав (Закон РФ "Об авторском праве и смежных правах": ст.146 УК РФ, ст.150 ГК РФ); информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (Федеральный закон "Об информации... "; ст.140 УК РФ); профессиональная (нотариальная, адвокатская) тайна (ст.51 УПК); медицинская (врачебная) тайна (ст.30 Основ законодательства Российской Федерации "Об охране здоровья граждан").

Законом также защищена конфиденциальная информация юридических лиц: коммерческая тайна (ст.139 ГК РФ; ст.183 УК РФ); банковская тайна (ст.183 УК РФ; ст.26 ФЗ РФ "О банках и банковской деятельности"); тайна связи (ст.1 ФЗ РФ "О почтовой связи"); служебная тайна (ст.139 ГК РФ).

Конфиденциальной объявляется информация, принадлежащая государству или его субъектам и их образованиям ("государственная конфиденциальная информация"). К ней относятся: служебная тайна (ст.139 ГК РФ); государственная тайна (Закон РФ "О государственной тайне"; ФЗ РФ "О федеральной фельдъегерской связи", ст.275, 276, 283, 284 УК РФ); данные предварительного следствия (ст.310 УК РФ); сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст.311 УК РФ); сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (ст.320 УК РФ).

Кроме перечисленных видов конфиденциальной информации, законом отнесены к таковой некоторые специальные разновидности сообщений независимо от воли их собственника. Например, ограничен порядок предоставления потребителю информации эротического содержания (ст.37 Закона РФ "О средствах массовой информации) и запрещена к распространению порнография (ст.242 УК РФ).

Указанный перечень не является исчерпывающим. Однако представляется, что дальнейшее его уточнение и дополнение будет происходить по мере развития криминалистической теории раскрытия и расследования преступлений в области информации на основе обобщения практики.

## 4. Конфиденциальность информации

Термин "нарушение целостности и конфиденциальности" широко используется в специальной литературе, в которой рассматривается проблема безопасности информационных систем, базирующихся на применении информационной техники. Специалисты обычно имеют в виду конкретные организационные и программно-технические меры, обеспечивающие защиту систем и сетей ЭВМ от действий, которые могут повлечь вредные последствия для хранящейся в памяти компьютеров информации. Говоря о целостности информации, подразумевают защиту данных от разрушения и изменения, в том числе и от вирусов. Конфиденциальность же понимается как предотвращение возможности использования информации лицами, которые не имеют к ней отношения. Появление вслед за специальной литературой и в законодательстве об информации термина "конфиденциальность" наряду с термином "тайна", по-видимому, оправданно[[6]](#footnote-6).

В словаре В. Даля слово "тайна" означает все сокрытое, неизвестное, неведомое или нечто скрываемое, секретное, не оглашаемое. Слово "конфиденциальный" означает "доверительный, не подлежащий огласке".

Как видно из сравнений смысла данных терминов, они обозначают одно и то же. Таким образом, тайна или конфиденциальность есть свойство документированной информации.

Конфиденциальная информация характеризуется доверительными отношениями, которые выражаются в передаче секретных сведений для определенной цели (в том числе для сохранения в тайне/ Использование подобной "доверительной" информации допускается только по ее целевому назначению. Обязанность сохранить конфиденциальную информацию в тайне вытекает из особой природы конфиденциальной информации и базируется во многом на нравственно-этических нормах и принципах, отражающих строго целевую направленность отношений по поводу использования конфиденциальной информации.

Признаками конфиденциальной информации являются секретность, неизвестность широкому кругу лиц, объективное выражение, идентифицированность, заинтересованность обладателя в сохранении сведений в тайне, доверительный характер, объясняющий строго целевое использование соответствующих сведений, возможность причинения морального и/или материального ущерба или нарушения интересов общества или государства в случае разглашения.

Режим секретности - установленный нормами права в нашей стране единый порядок обращения со сведениями, составляющими государственную и служебную тайны. Назначение: предотвращение утечки закрытой информации по агентурным каналам.

## 5. Государственная тайна

Государственная тайна как вид тайны неоднократно указывается в статьях Уголовного кодекса Российской Федерации и имеет непосредственное уголовно-правовое значение, связанное с обеспечением внешней безопасности государства и государственной безопасности в целом. Государственную тайну Российской Федерации составляют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. На основе сохранения неприкосновенности государственной тайны обеспечивается не просто "государственная безопасность" в широком понимании, а внешняя безопасность государства. Государственная тайна в уголовно-правовом отношении находится в основе комплекса двух интересов уголовно-правовой охраны: внешней безопасности государства и безопасности государства как таковой.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации "О безопасности" и включает Закон “О государственной тайне”, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

К государственной тайне могут быть отнесены следующие сведения:

1) сведения в военной области:

о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций.

2) сведения в области экономики, науки и техники:

* о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, мобилизационных мощностях промышленности по изготовлению вооружения и военной техники, об объемах поставок и о запасах стратегических видов сырья и материалов, а также о размещении и фактических размерах государственных материальных резервов;
* об использовании инфраструктуры Российской Федерации в интересах обеспечения ее обороноспособности и безопасности;
* о государственных запасах драгоценных металлов и драгоценных камней Российской Федерации, ее финансах и бюджетной политике (кроме обобщенных показателей, характеризующих общее состояние экономики и финансов).

3) сведения в области внешней политики и экономики:

о внешнеполитической и внешнеэкономической (торговой, кредитной и валютной) деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб ее интересам

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

о силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации.

Прекращение допуска к государственной тайне не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

## 6. Коммерческая тайна

В правовой обиход введены различные представления о тайне. Наряду с государственной, служебной, врачебной, коммерческой и иными вводится представление об адвокатской тайне, биржевой тайне, банковской тайне, налоговой тайне, тайне вклада и тайне договора, тайне телефонных переговоров и множества иных видов тайн.

В соответствии со статьей 2 Федерального закона "Об информации, информатизации и защите информации" под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Сведения должны быть известны или доверены узкому кругу лиц. При этом основанием известности сведений тому или иному лицу может быть профессиональная или служебная деятельность последних, семейно-брачные отношения и иное. Общим для всех видов конфиденциальных сведений является факт, что свободный доступ к ним ограничен в силу предписаний федерального законодательства. Нарушение неприкосновенности охраняемой законом тайны влечет юридическую (в том числе и уголовную) ответственность. На лицах, которым доверена такая информация, лежит правовая обязанность не нарушать ее конфиденциальность.

Уголовная ответственность за нарушение коммерческой и банковской тайны наступает при собирании сведений, составляющих коммерческую или банковскую тайну, в целях разглашения либо незаконного использования этих сведений, а также при незаконном разглашении или использовании сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца.

Одним из наиболее часто цитируемых нормативных правовых актов является статья 4 Федерального закона ”О коммерческой тайне” (О перечне сведений, которые не могут составлять коммерческую тайну) В документе сказано, что Правительство РФ постановляет что:

режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Определение сведений, составляющих коммерческую тайну, представляет собой одно из центральных звеньев в системе мер, осуществляемых предприятием по защите своей интеллектуальной собственности. Неправильное или несвоевременное выделение предмета защиты существенно снижает эффективность этой системы, либо вообще сводите ее на нет.

Критериями, по которым определяется информация, относимая к перечню сведений, составляющих коммерческую тайну предприятия, могут быть следующие:

* во-первых, эта информация должна быть коммерчески выгодной вам или выгодной для вашего конкурента в случае ее попадания в чужие руки. В качестве критерия важности конкретной информации принимается количественных показатель величины наносимого ущерба. То есть наиболее важной, с точки зрения безопасности предприятия, является информация, утечка которой, например, угрожает структурной целостности предприятия или способствует перекрытию каналов поступления материальных ресурсов;
* во-вторых, эта информация не должны быть общеизвестной или общедоступной на законных основаниях;
* в-третьих, эти сведения не должны являться государственными секретами или защищаться согласно нормам авторского или патентного права;
* в-четвертых, информация, составляющая коммерческую тайну, должна быть зафиксирована в письменной или иной материальной форме или находиться в исключительном ведении предприятия;
* в-пятых, такая информация должна быть понятным образом специально обозначена ("грифована") и в отношении нее должны быть обеспечены необходимые меры по сохранению конфиденциальности;
* в-шестых, эти сведения не должны напрямую касаться деятельности предприятия, способной нанести ущерб обществу, жизни и здоровью людей (нарушение законов, загрязнение окружающей среды и т.д.), а также использоваться в целях недобросовестной конкуренции, уклонения от налогообложения, осуществления запрещенной или незакрепленной в уставе предприятия деятельности.

## 7. Защита информации

Безопасность информации - это свойство (состояние) передаваемой, накапливаемой, обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды (человека и природы) и внутренних угроз, то есть ее конфиденциальность (секретность, смысловая или информационная скрытность), сигнальная скрытность (энергетическая и структурная) и целостность - устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам.

Под защитой информации, в более широком смысле, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Сущность защиты информации состоит в выявлении, устранении или нейтрализации негативных источников, причин и условий воздействия на информацию. Эти источники составляют угрозу безопасности информации. Цели и методы защиты информации (гл. II. - 1., II. - 2) отражают ее сущность.

В этом смысле защита информации отождествляется с процессом обеспечения информационной безопасности, как глобальной проблемы безопасного развития мировой цивилизации, государств, сообществ людей, отдельного человека, существования природы.

При этом понятие информационная безопасность характеризует состояние (свойство) информационной защищенности человека, общества, природы в условиях возможного действия угроз и достигается системой мер, направленных:

* на предупреждение угроз. Предупреждение угроз - это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
* на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
* на обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
* на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
* на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами

Предупреждение угроз возможно и путем получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

Обнаружение угроз - это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

Пресечение или локализация угроз - это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

* предотвращение разглашения и утечки конфиденциальной информации;
* воспрещение несанкционированного доступа к источникам конфиденциальной информации;
* сохранение целостности, полноты и доступности информации;
* соблюдение конфиденциальности информации;
* обеспечение авторских прав.

Учитывая вышесказанное защиту информации можно определить как совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов.

Защищаемая информация включает сведения, составляющие государственную, коммерческую, служебную и иные охраняемые законом тайны. Каждый вид защищаемой информации имеет свои особенности в области регламентации, организации и осуществления этой защиты.

Наиболее общими признаками защиты любого вида охраняемой информации являются следующие:

* защиту информации организует и проводит собственник или владелец информации или уполномоченные им на то лица (юридические или физические);
* защитой информации собственник охраняет свои права на владение и распоряжение информацией, стремится оградить ее от незаконного завладения и использования в ущерб его интересам;
* защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям.

Таким образом, защита информации - есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям.

Защищаемая информация, являющаяся государственной или коммерческой тайной, как и любой другой вид информации, необходима для управленческой, научно-производственной и иной деятельности. В настоящее время перед защитой информации ставятся более широкие задачи: обеспечить безопасность информации. Это обусловлено рядом обстоятельств, и в первую очередь тем, что все более широкое распространение в накоплении и обработке защищаемой информации получают ЭВМ, в которых может происходить не только утечка информации, но и ее разрушение, искажение, подделка, блокирование и иные вмешательства в информацию и информационные системы.

Следовательно, под защитой информации следует также понимать обеспечение безопасности информации и средств информации, в которых накапливается, обрабатывается и хранится защищаемая информация.

Таким образом, защита информации - это деятельность собственника информации или уполномоченных им лиц по:

* обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;
* предотвращению утечки и утраты информации;
* сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;
* сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Защита информации вызывает необходимость системного подхода; т.е. здесь нельзя ограничиваться отдельными мероприятиями. Системный подход к защите информации требует, чтобы средства и действия, используемые для обеспечения информационной безопасности организационные, физические и программно-технические рассматривались как единый комплекс взаимосвязанных, взаимодополняющих и взаимодействующих мер. Один из основных принципов системного подхода к безопасности информации - принцип "разумной достаточности", суть которого: стопроцентной защиты не существует ни при каких обстоятельствах, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы.

## 8. Угрозы конфиденциальности информации

Несанкционированный доступ - чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.

Для успешной защиты своей информации пользователь должен иметь абсолютно ясное представление о возможных путях несанкционированного доступа.

Ответственность за разглашение или использование коммерческой тайны по трудовому праву РФ рассматривается как один из видов юридической ответственности. Существует дисциплинарная и материальная ответственность за разглашение коммерческой тайны. Условия (основания) привлечения работника к материальной ответственности за разглашение коммерческой тайны, предусмотренные Трудовым кодексом РФ и Законом о коммерческой тайне (наличие соответствующего условия в трудовом договоре, ознакомление с положением о коммерческой тайне, допуск к коммерческой тайне и т.д.).

Действующее российское законодательство крайне противоречиво в вопросах о привлечении работника к ответственности за разглашение коммерческой тайны. С одной стороны, согласно ч.2 ст.139 ГК РФ работник, разгласивший служебную или коммерческую тайну вопреки трудовому договору, обязан возместить причиненные этим убытки (включая упущенную выгоду). С другой стороны, в соответствии со ст.238 ТК РФ размер материальной ответственности ограничен размерами реального ущерба, не включающего упущенную выгоду. Анализируются различные точки зрения по этому вопросу.

Но действительного ущерба при разглашении коммерческой тайны может не быть вообще, а весь ущерб может составить неполученная прибыль. Таким образом, имущественные интересы работодателя не могут считаться защищенными, даже если условие о сохранности служебной (коммерческой) тайны включить в трудовой договор. Следовательно, трудоправовая ответственность в данном случае несоразмерна содеянному и его последствиям и вряд ли будет достаточной.

Анализ действующего законодательства позволяет сделать вывод, что законодатель устанавливает неодинаковые подходы для разных категорий работников (работников и руководителей) к определению размеров и порядка возмещения убытков (ущерба), причиненного виновными действиями работников вследствие нарушения законодательства о коммерческой тайне, допуская в некоторых случаях привлечение работника по сути к гражданско-правовой ответственности.

Недостатки Закона о коммерческой тайне в том, что он обязывает работника не использовать коммерческую тайну в личных целях только в период существования трудовых правоотношений, отсутствие возможности привлечения к материальной или гражданско-правовой ответственности за нарушение указанной обязанности.

Использование работником или лицом, прекратившим трудовые отношения, коммерческой тайны в личных целях может причинить значительный ущерб обладателю коммерческой тайны, например, если работник использует коммерческую тайну для извлечения прибыли, в предпринимательской деятельности или для конкуренции с настоящим или бывшим работодателем.

Анализ действующего законодательства позволяет придти к выводу, что законодатель употребляет фразу "использование в личных целях" как минимум в двух смыслах:

1. как использование в корыстных целях, для извлечения прибыли;
2. как использование исключительно для себя без извлечения прибыли.

## 9. Меры по защите информации

Проблемы защиты информации занимают одно из ведущих мест в ряду приоритетных проблем, которые приходится разрешать субъектам хозяйственной деятельности.

Необходимость в защите информации возникла по следующим причинам:

- развитие информационных технологий привело к формированию открытого информационного общества;

- информация имеет непосредственную ценность в силу ее неизвестности третьим лицам, т.е. является товаром и подлежит защите;

- информация активно формирует новый уровень знаний, которые в виде умений и навыков персонала выступают основным фактором, обеспечивающим предприятию получение прибыли, и, следовательно, наряду с другими ресурсами подлежат защите;

- информация распространяется по формальным и неформальным каналам, что затрудняет ее защиту.

Информация в современном обществе – объект права и объект собственности. Процессы информатизации экономики обостряют противоречие между правом гражданина на доступ к информации и необходимостью ограничения этого права в целях защиты прав хозяйствующих субъектов. Как результат, установление правового режима информации и возможных форм ее использования, обеспечение защиты информации приобретает особое значение.

Основные направления обеспечения информационной безопасности бизнеса:

- защита информации о состоянии и движении материальных активов, чаще понимаемая как экономическая безопасность;

- защита информации о состоянии нематериальных активов и их носителях (персонале), определяемая как собственно информационная безопасность - защита средств хранения, обработки и передачи информации.

В качестве носителей информации выступают:

- открытая печать (газеты, журналы, реклама, отчеты);

- люди (персонал, друзья, родственники, знакомые);

- основные технические средства (телефон, факс, пейджер, радио, сотовый телефон, телевидение);

- вспомогательные технические средства (телевизоры, магнитофоны, диктофоны, пожарная и охранная сигнализация, офисная техника).

- официальные документы (указы, законы, постановления, приказы, руководства);

- деловые бумаги и архивы (справки, отчеты, договоры, рекламные проспекты);

- носители компьютерной информации (листинги, дискеты, магнитные ленты, СD, перфокарты);

- личные бумаги и архивы (дневники, письма, заметки, пометки);

- мусор (испорченные дискеты, копировальная бумага, использованные листинги).

Законодательством Российской Федерации установлено, что целями защиты являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;

- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных 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, имеющихся в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

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

Вышеизложенное позволяет сформулировать следующие условия формирования системы информационной безопасности организации:

1. Четкое определение понятия "система информационной безопасности" Обеспечить информационную безопасность – значит, осуществлять постоянную деятельность по выявлению, предупреждению, локализации и нейтрализации угроз потери, утечки информации и сведению к минимуму ущерба от реализации угроз.

2. Учет мнений и позиций собственника, акционеров, топ-менеджмента Мнения этих категорий лиц далеко не всегда совпадают.

3. Соблюдение принципов и алгоритма формирования системы информационной безопасности фирмы. В основе суждение: любое действие, нарушающее нормальное функционирование организации, понимается как угроза информационной безопасности фирмы.

# Заключение

В рыночно-конкурентных условиях возникает масса проблем, связанных с обеспечением безопасности не только физических и юридических лиц, их имущественной собственности, но и предпринимательской (коммерческой) информации, как вида интеллектуальной собственности. Для защиты предпринимательских информационных потоков от различного рода посягательств используются как правовые, так и специальные меры, а в необходимых случаях комплексное их применение.

Важно учитывать, что при охране своего права нельзя нарушать чужого (принцип эквивалентности), а также использовать незаконные средства охраны конфиденциальности информации. Несанкционированное использование или разглашение подобных сведений может причинить немалые убытки работодателю и другим законным обладателям конфиденциальной информации.

В целях устранения коллизий норм российского права необходимо распространить на коммерческую тайну, независимо от ее вида (коммерческая информация или ноу-хау) режим интеллектуальной собственности, что даст возможность поставить данные сведения на баланс организации в виде нематериальных активов и упростит процедуру определения размера ущерба.

Наконец, нужно установить ответственность за нарушение режима коммерческой тайны. Вид и форма ответственности может быть связаны либо с процедурой, нарушающей правомерный доступ к коммерческой тайне, либо с упущенной выгодой и моральным вредом.

Ответственность может наступать для субъекта, действия которого связаны с неправомерным нарушением процедуры защиты коммерческой тайны либо с причинением ущерба, только в случае, если коммерческая тайна была задокументирована на материальном носителе, а сам нарушитель был предупрежден о неправомерности своих действий. Умысел является главным доказательством вины. Правонарушение режима коммерческой тайны никогда не связано с неосторожностью или халатностью.

Установление стимулирующих выплат за допуск к коммерческой тайне и ее сохранение в виде надбавок позволит создать дополнительную материальную заинтересованность работника в сохранении коммерческой тайны, а также позволит работодателю более внимательно относиться к определению перечня сведений, составляющих коммерческую тайну и кругу лиц, имеющих к ней допуск.

Краткое рассмотрение пределов возможной защиты и сбора промышленной (коммерческой) информации свидетельствует о недостаточной пока правовой проработке данной проблемы. Однако значение и учет в предпринимательской деятельности действующего законодательства позволяют избежать серьезных ошибок и не вступать в конфликт с законом.

# Список использованной литературы

1. Конституция Российской Федерации. – М., 2006.

2. Гражданский кодекс Российской Федерации. Части первая и вторая. - М., 2003.

3. Уголовный кодекс Российской Федерации. - М., 2002.

4. Бачило И.Л. Интеллектуальная: собственность - объект современного права. - М., 2000.

5. Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 19 августа 1993 г., N 33.

6. Долгополов Ю.Б. Предпринимательство и безопасность. – М., 2000.

7. Казакевич О.Ю. и др. Предприниматель в опасности: способы защиты (практическое руководство для предпринимателей и бизнесменов). - М., 2001.

8. Кавеладзе И.Т. Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации). - М., 1992.

9. Раевский Г. Угрозы экономической безопасности предприятия и задачи службы безопасности по их нейтрализации // Частный сыск № 4. М., 1994

10. Сергиенко Л.А. Правовая защита персональных данных. Цели и принципы правового регулирования // Проблемы информатизации. 1995 Вып. 1-2.

1. Ч.1. ст.2. ГК РФ. [↑](#footnote-ref-1)
2. Ст.2 ФЗ "Об информации, информатизации и защите информации". [↑](#footnote-ref-2)
3. Бакут П.А., Шумилов Ю.П. //Информационные ресурсы России. 1999г. № 3. [↑](#footnote-ref-3)
4. Бачило И.Л. Интеллектуальная: собственность — объект современного права. М., 2000 С 45. [↑](#footnote-ref-4)
5. Ст. 2 Федерального закона от 20.02.95 № 24-ФЗ "Об информации, информатизации и защите информации". [↑](#footnote-ref-5)
6. Сергиенко Л. А. Правовая защита персональных данных. Цели и принципы правового регулирования //Проблемы информатизации — 1995. Вып.1. С.51. [↑](#footnote-ref-6)