# Тема 6. Правовые режимы защиты информации конфиденциального характера.

***Понятие информации конфиденциального характера по российскому законодательству и ее основные виды: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства. Основные методы правового регулирования конфиденциальной информации. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов «конфиденциальной» информации (дисциплинарная, гражданско-правовая, административная и уголовная).***

**6.1. Понятие информации конфиденциального характера по российскому законодательству и ее основные виды: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.**

Единое понятие конфиденциальной информации в действующем законодательстве отсутствует. Согласно утратившему силу *ФЗ РФ «Об участии в международном информационном обмене»* (*абз. 2, ст. 2*) **конфиденциальной** считается документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. **Документированной** является информация (документ), зафиксированная на материальном носителе соответствующим установленной форме (наличие необходимых реквизитов, позволяющих ее идентифицировать) (*абз. 1 ст. 2 ФЗ РФ «Об участии в международном информационном обмене»*).

В *п. 7 ст. 2* *действующего ФЗ РФ «Об информации, информационных технологиях и защите информации»* дается определение **конфиденциальности информации** как обязательного для выполнения лицом, получившим доступ к определенной информации, требования не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальная информация в любых ее формах и видах тщательно охраняется законом от несанкционированного доступа к ней посторонних лиц. Поэтому последствия разглашения таких сведений более чем серьезны – вплоть до уголовной ответственности, которая в том числе выражается и в лишении свободы.

*Статья 5* *закона «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ* подразделяет любые сведения, находящиеся в распоряжении граждан, госорганов и юридических лиц, на общедоступные и данные с ограниченным или запрещенным доступом.

Конфиденциальными могут быть сведения с ограниченным доступом.

Важно: доступ к каким-либо информационным объектам может ограничиваться или запрещаться исключительно в соответствии с федеральным законом.

Тайны бывают разные. Тайна в широком смысле этого слова – конфиденциальная информация, распространение которой возможно лишь в определенных ситуациях.

Информация – это сведения (сообщения, данные) независимо от формы их представления (*п. 1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»* (далее – ФЗ)).

Иными словами, **информация** – это не только документы или файлы с какими-то данными. Информация – это все, что нас окружает: услышанное на переговорах и совещаниях, увиденное в документах на различных носителях – как материальных, так и электронных, написанное собственноручно или напечатанное с помощью технических средств, нарисованное или начерченное в любом виде и пр.

То есть то, что мы видим, слышим, созерцаем, и есть информация, представленная в самых разнообразных формах. В зависимости от того, к какой сфере относится информация, требующая соблюдения конфиденциальности, выделяют следующие виды тайн: государственную, коммерческую, налоговую, военную, личную, семейную, телефонных переговоров (почтовых, телеграфных и иных сообщений), служебную, банковскую, страхования, завещания, усыновления (удочерения), следствия, голосования, нотариальную, адвокатскую, врачебную и др.

Поскольку нас интересует соблюдение тайны работниками организации, перечислим виды тайн (с указанием НПА, их регулирующих), которые чаще всего встречаются в организациях:

– государственная тайна (*ст. 5 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»*, Перечень сведений, отнесенных к государственной тайне);

– коммерческая тайна (*ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»*);

– персональные данные (*ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»*);

– банковская тайна (*ч. 2, ст. 857 Гражданского кодекса РФ, ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности», ст. 57 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»*);

– врачебная тайна (*ст. 13, 92 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», ст. 15 Семейного кодекса РФ от 29.12.1995 № 223-ФЗ, ст. 9 Закона РФ от 02.07.1992 № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании», ст. 13 Федерального закона РФ от 20.07.2012 № 125-ФЗ «О донорстве крови и ее компонентов», ст. 14 Закона РФ от 22.12.1992 № 4180-1 «О трансплантации органов и (или) тканей человека»*);

– тайна страхования (*ч. 2, ст. 946 ГК РФ, ст. 47 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», ст. 18.2 Федерального закона от 24.07.1998 № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»*);

– тайна связи *(ст. 23 Конституции Российской Федерации, ст. 53, 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», ст. 15 Федерального закона от 17.07.1999 № 176-ФЗ «О почтовой связи»*); информация о содержании корпоративного договора, заключенного участниками непубличного общества (*ч. 1, ст. 67.2 ГК РФ*);

– информация о новых решениях и технических знаниях, если она получена сторонами по договору подряда (*ч. 2, ст. 727 ГК РФ*);

– сведения, касающиеся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами (ч. 2, ст. 771 ГК РФ);

– секрет производства (ноу-хау) (ч. 4, ст. 1465 ГК РФ).

## Виды конфиденциальной информации:

Все виды сведений, сохранность которых защищается на законодательном уровне, перечислены в одноименном перечне, утвержденном *Указом Президента России от 06.03.1997 № 188*.

1. П**ерсональные** [**данные**](https://nsovetnik.ru/files/20151208persdannie.doc) **гражданина** – любые сведения о событиях, фактах и обстоятельствах его частной жизни;

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с *федеральными законами от 20 апреля 1995 г.*[*N 45-ФЗ*](http://www.consultant.ru/document/cons_doc_LAW_219120/cabdcbeac2293f92b2860d54e3858f7c59da1256/#dst100057)*«О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г.*[*№ 119-ФЗ*](http://www.consultant.ru/document/cons_doc_LAW_212439/f39c81317cefe51924c1ecc98a5c3decbbac114c/#dst100061)*«О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»*, другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. **Служебная тайна** представляет собой служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским [кодексом](http://www.consultant.ru/document/cons_doc_LAW_300822/#dst0) Российской Федерации и федеральными законами.

4. **Профессиональная тайна** – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с [Конституцией](http://www.consultant.ru/document/cons_doc_LAW_2875/2573feee1caecac37c442734e00215bbf1c85248/#dst100094) Российской Федерации и федеральными законами ([врачебная](http://www.consultant.ru/document/cons_doc_LAW_319676/9f906d460f9454a8a0d290738d9fc2798c1e865a/#dst100102), [нотариальная](http://www.consultant.ru/document/cons_doc_LAW_304349/827a0570bc7a51eb7e0951ca313b4b7b629cb94f/#dst58), [адвокатская](http://www.consultant.ru/document/cons_doc_LAW_221313/afe346a9065e891a762908c86e6de63f45533e19/#dst100078) тайна, [тайна](http://www.consultant.ru/document/cons_doc_LAW_314853/2add28425adfc0411d61abad9deab4873e7ad274/#dst100594) переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. **Коммерческая тайна** представляет собой сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с *Гражданским*[*кодексом*](http://www.consultant.ru/document/cons_doc_LAW_298678/f8743d677137889f4c521c9e3e17a5d837ed54bf/#dst101423) *Российской Федерации* и федеральными [законами](http://www.consultant.ru/document/cons_doc_LAW_296152/#dst0).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с *Федеральным* [*законом*](http://www.consultant.ru/document/cons_doc_LAW_319690/1c194590ac1e7f7d1f67e084b018deaae29bcdef/#dst31) *от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве»*.

**6.2. Основные методы правового регулирования конфиденциальной информации**.

1. Установление понятия конфиденциальной информации.

2. Установление сведений, которые составляют конфиденциальную информацию (согласно *ст. 857 ГК* банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте).

# 3. Установление сведений, которые не могут составлять конфиденциальную информацию (в *постановлении Правительства РФ «Об утверждении Порядка назначения и выплаты ежемесячных компенсационных выплат отдельным категориям граждан» от 03.11.1994* определен перечень сведений, которые не м.б. отнесены к разряду служебной информации ограниченного распространения, в частности, акты законодательства, сведения о чрезвычайных ситуациях, описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес, порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц).

# 4. Установление порядка предоставления конфиденциальной информации государственным органам. Согласно *ФЗ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»* обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

5. Установление запрета действий, которые могут привести к нарушению режима конфиденциальной информации. Согласно *ФЗ от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»* адвокат не м.б. вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

**6.3. Основные требования, предъявляемые к организации защиты конфиденциальной информации** (КИ).

Под **разглашением КИ** понимаются умышленные или неосторожные действия допущенных к КИ лиц, приведшие к преждевременному, не вызванному служебной необходимостью распространению указанной информации среди лиц, включая работников АО, которым эта информация не была доведена в официально установленном порядке.

**Утечка конфиденциальной информации** – это несанкционированное распространение информации за пределы установленного физического пространства.

Комплексная защита КИ имеет целью решение двух задач:

1) защиту права организации на КИ, в том числе относящуюся к категории интеллектуальной собственности организации (достигается на основе применения правовых норм действующего законодательства РФ);

2) предотвращение угроз информационной безопасности организации, их выявление и существенное ослабление (достигается на основе реализации совокупности согласованных по цели, месту и времени применения правовых, организационных и технических мер защиты КИ, образующих систему защиты конфиденциальной информации (СЗКИ)).

СЗКИ дает возможность укрепления экономической безопасности организации, что способствует созданию условий для долгосрочного устойчивого функционирования организации.

Создание системы защиты КИ

Для того чтобы легально заниматься защитой конфиденциальной информации нужно получить лицензию на право осуществления деятельности по технической защите конфиденциальной информации (В соответствии с Положением «О лицензировании деятельности по технической защите конфиденциальной информации», *утвержденным Постановлением Правительства Российской Федерации от 30 апреля 2002 г. № 290*):

Для этого нужно выполнить следующие требования:

– осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности "компьютерная безопасность", "комплексное обеспечение информационной безопасности автоматизированных систем" или "информационная безопасность телекоммуникационных систем", либо специалистами, прошедшими переподготовку по вопросам защиты информации;

– соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами Российской Федерации и нормативно-методическими документами по технической защите информации; (*пп. "б" в ред. Постановления Правительства РФ от 23.09.2002 N 689*);

– использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

– использование третьими лицами программ для электронно-вычислительных машин или баз данных на основании договора с их правообладателем.

Для получения лицензии соискатель лицензии представляет в лицензирующий орган следующие документы:

– заявление о выдаче лицензии с указанием: лицензируемой деятельности; наименования, организационно-правовой формы и места нахождения – для юридического лица; фамилии, имени, отчества, места жительства, данных документа, удостоверяющего личность, – для индивидуального предпринимателя;

– копии учредительных документов и документа, подтверждающего внесение записи о юридическом лице в Единый государственный реестр юридических лиц;

– копия свидетельства о государственной регистрации соискателя лицензии – индивидуального предпринимателя;

– копия свидетельства о постановке соискателя лицензии на учет в налоговом органе с указанием идентификационного номера налогоплательщика;

– документ, подтверждающий уплату лицензионного сбора за рассмотрение заявления о выдаче лицензии;

– сведения о квалификации специалистов по защите информации соискателя лицензии.

Если копии документов не заверены нотариально, вместе с копиями предъявляются оригиналы.

Срок действия лицензии составляет пять лет и может быть продлен по заявлению лицензиата в порядке, предусмотренном для переоформления лицензии.

Переоформление лицензии осуществляется в течение десяти дней со дня получения лицензирующим органом соответствующего заявления.

Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации.   
Как Известно, право — это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определённых сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовые нормы обеспечения безопасности и защиты информации на любом предприятии (фирме, организации) отражаются в совокупности учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и защиты информации отражаются в Уставе:

* предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;
* предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

* создавать организационные структуры по защите конфиденциальной информации;
* издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
* включать требования по защите информации в 5; договоры по всем видам хозяйственной деятельности;
* требовать защиты интересов предприятия со стороны государственных и судебных инстанций;
* распоряжаться информацией, являющейся собственностью предприятия, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств с производства;
* разработать «Перечень сведений конфиденциальной информации». Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре.

Устав организации должен содержать следующие требования:

Раздел «Права и обязанности»:

1. Фирма имеет право:

* обеспечивать свою экономическую безопасность, определять состав, объем и порядок защиты конфиденциальной информации;
* требовать от сотрудников обеспечения экономической безопасности и защиты конфиденциальной информации;
* осуществлять контроль за соблюдением мер обеспечения экономической безопасности и защиты конфиденциальной информации.

2. Фирма обязана:

* обеспечить экономическую безопасность и сохранность конфиденциальной информации;
* осуществлять действенный контроль выполнения мер экономической безопасности и защиты конфиденциальной информации.

Раздел «Конфиденциальная информация»:

Общество организует защиту своей конфиденциальной информации. Состав и объем сведений конфиденциального характера, и порядок их защиты определяются генеральным директором.

ВНЕСЕНИЕ ЭТИХ ДОПОЛНЕНИЙ ДАЕТ ПРАВО АДМИНИСТРАЦИИ:

* создавать организационные структуры по защите коммерческой тайны или возлагать эти функции на соответствующих должностных лиц;
* издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;
* включать требования по защите коммерческой тайны в договоры по всем видам хозяйственной деятельности (коллективный и совместные со смежниками);
* требовать защиты интересов фирмы перед государственными и судебными органами;
* распоряжаться информацией, являющейся собственностью фирмы, в целях извлечения выгоды и недопущения экономического ущерба коллективу и собственнику средств производства.

Коллективный договор должен содержать следующие требования:

Раздел «Предмет договора»

* Администрация обязуется в целях недопущения нанесения экономического ущерба коллективу обеспечить разработку и осуществление мероприятий по экономической безопасности и защите конфиденциальной информации.
* Трудовой коллектив принимает на себя обязательства по соблюдению установленных на фирме требований по экономической безопасности и защите конфиденциальной информации.
* Администрации учесть требования экономической безопасности и защиты конфиденциальной информации в правилах внутреннего трудового распорядка, в функциональных обязанностях сотрудников и положениях о структурных подразделениях.

Раздел «Кадры. Обеспечение дисциплины труда»

Администрация обязуется нарушителей требований по экономической безопасности и защите конфиденциальной информации привлекать к ответственности в соответствии с законодательством РФ.

Правила внутреннего трудового распорядка для рабочих и служащих предприятия целесообразно дополнить следующими требованиями:

Раздел «Порядок приема и увольнения рабочих и служащих»

При приеме сотрудника на работу или при переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией, а также при увольнении администрация обязана:

* проинструктировать сотрудника о правилах экономической безопасности и сохранения конфиденциальной информации;
* оформить письменное обязательство о неразглашении конфиденциальной информации. Администрация вправе:
* принимать решения об отстранении от работы лиц, нарушающих требования по защите конфиденциальной информации;
* осуществлять контроль за соблюдением мер по защите и неразглашении конфиденциальной информации в пределах предприятия.

Раздел «Основные обязанности рабочих и служащих»

Рабочие и служащие обязаны:

* знать и строго соблюдать требования экономической безопасности и защиты конфиденциальной информации;
* дать добровольное письменное обязательство о неразглашении сведений конфиденциального характера;
* бережно относиться к хранению личных и служебных документов и продукции, содержащих сведения конфиденциального характера. В случае их утраты немедленно сообщить об этом администрации.

Раздел «Основные обязанности администрации»

Администрация и руководители подразделений обязаны:

* обеспечить строгое соблюдение требований экономической безопасности и защиты конфиденциальной информации;
* последовательно вести организаторскую, экономическую и воспитательную работу, направленную на защиту экономических интересов и конфиденциальной информации;
* включать в положения о подразделениях и должностные инструкции конкретные требования по экономической безопасности и защите конфиденциальной информации;
* неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других хозяйственных и организационных документов в части обеспечения экономической безопасности и защиты конфиденциальной информации.

Администрация и руководители подразделений несут прямую ответственность за организацию и соблюдение мер по экономической безопасности и защите конфиденциальной информации.

В договоре о проведении совместных работ должны содержаться следующие требования: Раздел «Условия конфиденциальности»

Стороны обязуются не передавать лицензии лицам и не раскрывать публично сведения о проводимых совместно работах без взаимного согласования. За нарушение данного условия стороны несут финансовую ответственность по возмещению убытков, упущенной выгоды и морального ущерба.

Лица, нарушившие условия конфиденциальности, могут быть привлечены к ответственности в соответствии с действующим законодательством.

Обязательства конкретного сотрудника, рабочего или служащего в части защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с *КЗоТ (гл. III*) при заключении трудового договора трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора (*КЗоТ РФ ст. 18*).

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.

Использование договоров о неразглашении тайны — вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Дальше задача — не допустить утраты коммерческих секретов.

Реализация правовых норм и актов, ориентированных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права.

**Конфиденциальность** – это форма обращения со сведениями, составляющими конфиденциальную информацию, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.

**Договоры** – это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.

**Обязательство** – гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия.

Правовое регулирование необходимо для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления задач и правомочий отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных интересов граждан и организаций.

Анализ законодательства, регулирующего деятельность субъектов в сфере информационной безопасности, показывает наличие определенных недостатков. Существующие правовые нормы разбросаны по различным нормативным актам, издававшимся в разное время, в разных условиях и на разных уровнях. Действующее законодательство не систематизировано, что создает большие трудности в его использовании на практике.

**Организационная защита** — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

* организацию охраны, режима, работу с кадрами, с документами;
* использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно- технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

К основным организационным мероприятиям можно отнести:

* организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;
* организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерам] ответственности за нарушение правил защиты ин формации и др.;
* организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
* организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
* организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.
* организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, и выполнение, возврат, хранение и уничтожение;

Исходя из ситуации и в целях совершенствования системы защиты информации я предлагаю объединить все службы занимающиеся защитой информации в одну службу и назвать её службой безопасности, функции которой будут следующими:

* организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, арендаторами, партнерами и посетителями;
* руководит работами по технической защите, а так же по правовому и организационному регулированию отношений по защите государственной тайны и конфиденциальной информации;
* разрабатывает основополагающие документы с целью закрепления в них требований обеспечения безопасности и защиты государственной тайны и конфиденциальной информации, в частности устава, правил внутреннего трудового распорядка, положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
* разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся государственной тайны и конфиденциальной информации, при всех видах работ организует и контролирует выполнение требований инструкции по защите государственной тайны и конфиденциальной информации;
* изучает все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки государственной тайны и конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций в отношении деятельности организации и е клиентов, партнеров, смежников;
* организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности организации;
* разрабатывает, ведет, обновляет и пополняет перечень сведений, составляющих конфиденциальную информацию и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
* обеспечивает строгое выполнение требований нормативных документов по защите конфиденциальной информации;
* осуществляет руководство службами и подразделениями безопасности предприятий организации в части оговоренных в договорах условий по защите государственной тайны и конфиденциальной информации;
* организует и регулярно проводит учебу сотрудников фирмы и службы безопасности по всем направлениям защиты государственной тайны и конфиденциальной информации, добиваясь, чтобы к охране коммерческих секретов был глубоко осознанный подход;
* ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение государственной тайны и конфиденциальной информации;
* ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

Служба безопасности должна быть самостоятельной организационной единицей, подчиняющейся непосредственно генеральному директору организации.

Возглавляет службу безопасности начальник службы в должности заместителя генерального директора по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

* отдела охраны;
* Отдел по защите конфиденциальной информации:
* Сектор обработки документов с грифом "конфиденциальная информация";
* лаборатории контроля защищенности от НСД к информации автоматизированных систем и средств вычислительной техники.
* Лаборатория комплексного контроля эффективности противодействия иностранным техническим разведкам и технической защиты информации ;
* группа анализа возможности образования технических каналов утечки информации;

Для защиты конфиденциальной информации разрабатываются в организации должны быть разработаны следующие нормативно-правовые документы:

* Перечень сведений, составляющих конфиденциальную информацию организации;
* Договорное обязательство о неразглашении КИ
* Инструкция по защите конфиденциальной информации

Защита информации в компьютерах должна осуществляться в соответствии с требования РД ГостехКомиссии, и СТР-к (специальные требования и рекомендации по технической защите конфиденциальной информации).

В первую очередь следует разработать перечень сведений, составляющий конфиденциальную информацию организации. В перечень должны включаться все сведения, являющиеся собственностью организации.

Под сведениями (и их носителями) понимаются:

* Данные, полученные в результате обработки информации с помощью технических средств (оргтехники);
* Информация как часть данных, несущая в себе полезные сведения и используемая сотрудниками организации для работы в служебных целях;
* Документы (носители), образующие в результате мыслительной деятельности сотрудников организации, включающие в себя сведения любого происхождения, вида и назначения, но необходимые для нормального функционирования организации.

Сведения, включенные в Перечень, имеют ограниченный характер на использование (применение). Ограничения, вводимые на использования сведений, составляющих конфиденциальную информацию, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при организации трудовой деятельности работников (персонала) её подразделений, а также при их сотрудничестве с работниками других предприятий.

В совокупности под конфиденциальной информацией надо понимать сведения, не являющиеся государственными секретами, но которые связаны, прежде всего, с производственной, управленческой, финансовой или другой экономической деятельностью организации, разглашение (передача, утечка, хищение) которой может нанести ущерб её интересам или интересам их владельцев.

Законодательной основой защиты конфиденциальной информацией является часть вторая ГК РФ.

При разработки перечня следует руководствоваться:

* Конституцией РФ, принятой 12 декабря 1993 года
* Законом РФ “ О государственной тайне ” № 5485-1 от 21.07.93
* Федеральным законом РФ “ Об информации, информатизации и защите информации” № 24-ФЗ от 20.02.95
* Указом Президента РФ “об утверждении Перечня сведений, отнесённых к государственной тайне” № 1203 от 30.11.95
* Указом Президента РФ “об утверждении Перечня сведений, конфиденциального характера” № 188 от 06.03.97
* Постановлением Правительства РФ “ о Перечне сведений, которые не могут составлять коммерческую тайну” № 35 от 05.12.91
* Сведения, являющиеся общедоступными на законных основаниях, в том числе в соответствии с Постановлением Правительства РФ № 35 от 05.12.91.:
* Учредительные документы (решение о создании предприятия или договор учредителей) и устав;
* Документы, дающие право заниматься предпринимательской деятельности (регистрационные удостоверения, лицензии, патенты);
* Сведения по установленным формам отчётности о финансово- хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему России;
* Документы о платежеспособности; сведения о численности, составе работающих, их заработной плате и условиях труда, а так же о наличии свободных рабочих мест;
* Документы об уплате налогов и обязательных платежах;
* Сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а так же других нарушениях законодательств РФ и размерах причиненного при этом ущерба;
* Сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах и других организациях, занимающихся предпринимательской деятельностью.
* Анализом преимуществ и недостатков для работы открытым и закрытым ( внутренним) применением таких сведений.
* Анализом характера возможного ущерба в случае несанкционированного распространения сведений конфиденциального;

После разработки проекта перечня, он обсуждается и утверждается на ЭТК и согласовывается с генеральным директором организации, начальниками основных служб и отделов Перечень вводится приказом генерального директора организации в виде приложения к нему.

Сотрудники организации, допускаемые по роду своей работы или функциональным обязанностям к сведениям, составляющим конфиденциальную информацию, должны под расписку ознакомится с этим приказом и приложением к нему.

Перечень дифференцированно должен доводиться не реже 1 раза в год до всех сотрудников организации, которые используют в своей работе частично или в полном объёме сведения, информацию, данные или работают с документами ДСП и их носителями. Все лица принимаемы на работу в организацию, должны пройти инструктаж и ознакомиться с памяткой о сохранении конфиденциальной информации.

Сотрудник, получивший доступ к конфиденциальной информации и документам, должен подписать индивидуальное письменное договорное обязательство ( приложение 2 ) об их неразглашении. Обязательство составляется в одном экземпляре и хранится в личном деле сотрудника не менее 5 лет после его увольнения. При его увольнении из организации ему даётся подписка о неразглашении конфиденциальной информации организации.

Далее должна быть разработана инструкция, регламентирующая порядок доступа сотрудников к КИ, порядок создания, учёта, хранения и уничтожения конфиденциальной документов организации. При написании такой инструкции следует руководствовать положениями ГОСТа Р6 30-2003- “ Унифицированные системы документации.”, а так же “ Унифицированная система организационно-распорядительной документации. Требования к оформлению документов”, который был принят и введен в действие постановлением Госстандарта РФ от 3 марта 2003 г. N 65-ст.

Инструкция по защите конфиденциальной информации должна состоять из следующих частей:

1. ОБЩИЕ ПОЛОЖЕНИЯ.
2. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ
3. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
4. СИСТЕМА ДОСТУПА СОТРУДНИКОВ К СВЕДЕНИЯМ СОСТАВЛЯЮЩИМ КИ.
5. КРУГ ЛИЦ, ИМЕЮЩИХ ПРАВО ДАВАТЬ РАЗРЕШЕНИЕ НА ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ
6. ПОРЯДОК ОФОРМЛЕНИЯ РАЗРЕШЕНИЯ НА ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ
7. ПОРЯДОК ДОСТУПА НА СОВЕЩАНИЯ ПО ВОПРОСАМ, СОДЕРЖАЩИМ КОНФИДЕНЦИАЛЬНЫЕ СВЕДЕНИЯ
8. ПОДГОТОВКА И ИЗДАНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ
9. УЧЕТ, ПРОХОЖДЕНИЕ И ОТПРАВЛЕНИЕ ИЗДАННЫХ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ
10. ПРИЕМ, УЧЕТ И ПРОХОЖДЕНИЕ ПОСТУПИВШИХ ДОКУМЕНТОВ
11. УЧЕТ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ ВЫДЕЛЕННОГО ХРАНЕНИЯ
12. УЧЕТ ЖУРНАЛОВ И КАРТОТЕК
13. ОРГАНИЗАЦИЯ ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ
14. ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ КОНТРОЛЯ ИСПОЛНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ
15. РАЗМНОЖЕНИЕ ДОКУМЕНТОВ
16. УНИЧТОЖЕНИЕ ДОКУМЕНТОВ
17. СОСТАВЛЕНИЕ И ОФОРМЛДЕНИЕ НОМЕНКЛАТУРЫ ДЕЛ С ГРИФОМ «КОНФИДЕНЦИАЛЬНО»
18. ФОРМИРОВАНИЕ И ОФОРМЛЕНИЕ ДЕЛ
19. ПРОВЕРКА НАЛИЧИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ.
20. ПОДГОТОВКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ НА АРХИВНОЕ ХРАНЕНИЕ
21. ПОРЯДОК ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ В АРХИВ
22. ПРИЛОЖЕНИЯ

Защита КИ является одним из важнейших факторов создания предпосылок для стабильного существования и прогрессивного развития организации.

Основными условиями обеспечения информационной безопасности организации в контексте намеченного подхода к решению задач защиты КИ являются:

* построение моделей злоумышленников и конкурентов на основе поиска и аутентификации информации о их намерениях и устремлениях;
* определение перечня сведений, составляющих объект защиты интересов концерна в конкретных областях его деятельности;
* формирование предпочтительной для концерна структуры системы защиты КИ на основе синтеза, структурной оптимизации и технико-экономической оценки альтернативных вариантов СКЗКИ;
* управление процессом реализации избранного замысла защиты КИ и координация работ по организации защиты КИ между всеми заинтересованными структурными подразделениями организации;
* совмещение организационно-административных мер защиты КИ с активными вовлечением в указанный процесс всего персонала организации;
* введение персональной ответственности (в том числе и материальной) должностных лиц всех уровней, а также других работников концерна, допущенных к КИ, за обеспечение установленного в АО режима конфиденциальности.

Вышеперечисленные документы разработаны с учетом общих требований к содержанию и оформлению подобных документов.

Разработанные автором документы вы можете получить, для этого достаточно отправить просьбу об получении такой инструкции мне на e-mail указав название организации, область деятельности ).

**6.4. Юридическая ответственность за нарушения правовых режимов «конфиденциальной» информации (дисциплинарная, гражданско-правовая, административная и уголовная).**

Все виды конфиденциальной информации регламентируются различными нормативными актами (искл. – коммерческая информация, которая с 2004 года регламентируется специальным законом).

Вся информация, отнесенная к категории конфиденциальной может использоваться только с согласия правообладателя.

За разглашение конфиденциальной информации законами РФ предусмотрено 3 вида ответственности:

* дисциплинарная;
* административная;
* уголовная.

**Дисциплинарная** ответственность варьируется от устного замечания до увольнения и применяется исключительно по результатам служебной [проверки](https://nsovetnik.ru/files/20151208prikaz.doc), в ходе которой должна быть установлена причастность работника к утечке сведений, а также его вина в этом.

**Административное** наказание наступает за разглашение любого вида конфиденциальной информации и, согласно *статье 13.14 КоАП РФ*, представляет собой штраф в размере от 500 до 1 000 рублей для рядовых граждан и от 4 000 до 5 000 рублей для работников, наделенных организационно-распорядительными полномочиями, то есть должностных лиц.

**Уголовное** законодательство относится к ответственности за нарушение режима конфиденциальности более избирательно – она применяется при условии разглашения коммерческой, банковской или налоговой тайны. При этом сбор таких сведений, согласно статье *183 УК РФ*, должен осуществляться заведомо незаконными путями – посредством подкупа, угроз, хищения документов и т. д.

Наказание зависит от обстоятельств преступления и его последствий – от штрафа до 500 000 рублей до 7 лет тюрьмы.

*Статья 183* – не единственная норма УК РФ, предусматривающая ответственность за разглашение конфиденциальных сведений. Например, раскрытие информации о фирме, повлекшее падение стоимости ее акций (инсайдерской информации), подпадает под действие *статьи 185.6 УК РФ* и грозит виновному немалыми штрафами – от 300 000 до 1 000 000 рублей, а также запретом на замещение определенных должностей в течение 4 лет.

Кроме того, параллельно с любым видом наказания может быть рассмотрен вопрос о привлечении лица, допустившего утечку информации с ограниченным доступом, к гражданско-правовой ответственности. Речь идет об обязанности возместить вред, причиненный в результате разглашения сведений, – как материальный, так и моральный.

**Рекомендуемая литература**:

1. Столяров Н.В. Разработка системы защиты конфиденциальной информации. – Режим доступа: <http://www.bre.ru/security/20864.html>.

2. Годнева Т.Ю., Котова К.А., Лисова С.Ю. Правоведение: учебное пособие. – ГОУВПО «Ивановский государственный энергетический университет имени В.И. Ленина». – Иваново, 2008. – 204 с. – Режим доступа: <http://txtb.ru/40/index.html>.

3. Нормативно-правовые акты, указанные в тексте

**Контрольные вопросы:**

1. Что собой представляет КИ?

2. Каким образом законодатель регламентирует понятие «КИ»?

3. Что собой представляет документированная информация?

4. Что означает конфиденциальность информации?

5. Назовите сведения, причисляемые к конфиденциальным?

6. Каким нормативным правовым актом (НПА) установлен перечень конфиденциальных сведений?

7. Назовите виды тайн, которые должны соблюдаться соответствующими работниками?

8. Что собой представляют персональные [данные](https://nsovetnik.ru/files/20151208persdannie.doc) гражданина?

9. Что собой представляет служебная тайна?

10. Что собой представляют коммерческая тайна?

11. Назовите основные методы правового регулирования конфиденциальной информации.

12. Что означает утечка конфиденциальной информации?

13. Что означает разглашение КИ?

14. Назовите задачи комплексной защиты КИ.

15. Какие требования предъявляются к субъекту, который занимается защитой КИ?

16. Что необходимо для получения лицензии на ведение деятельности по защите КИ?

17. Какие документы должен представить соискатель лцензии в лицензирующий орган?

18. Назовите субъектов, которые занимаются разработкой мер по заите информации.

19. В каком нормативном документе фиксируются требования по защите информации?

20. Опишите и охарактеризуйте структуру Устава организации.

21. Что означает понятие «организационная защита»?

22. Что обеспечивает организационная защита?

23. Назовите основные организационные мероприятия по защите информации.

24. Опишите полномочия Службы безопасности.

25. Назовите организационную структуру службы безопасности.

26. Назовите нормативно-правовые документ организации, необходимые для защиты конфиденциальной информации.

27. Перечислите источники права в сфере организации и обеспечения защиты информации.

28. Назовите структурные элементы Инструкция по защите конфиденциальной информации.

29. Назовите основные условия обеспечения информационной безопасности организации.

30. Назовите виды юридической ответственности за нарушения правовых режимов «конфиденциальной» информации и охарактеризуйте их.