НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕТЫ ДЛЯ ОБЕСПЕЧНИЯ КСЗИ

20501 Урюмцев Илья

Значение нормативно-методического обеспечения

- В целях обеспечения комплексного подхода к формированию законодательства по проблемам защиты информации и информатизации в России в апреле 1992 г. была утверждена «Программа подготовки законодательного и нормативного обеспечения работ в области информатизации и защиты информации». В соответствии с этой Программой была намечена разработка базового Закона РФ в области информатизации «Об информации, информатизации и ЗИ», а также еще ряда специальных законов

Нормативно-методическое обеспечение КСЗИ представляет собой комплекс положений законодательных актов, нормативов, методик, правил, регламентирующих создание и функционирование КСЗИ, взаимодействие подразделений и лиц, входящих в структуру системы, а также статус органов, обеспечивающих функционирование КСЗИ

Требования к документам

Нормативные документы, определяющие порядок защиты, должны удовлетворять следующим требованиям:

- — соответствовать структуре, целям и задачам предприятия;
- — описывать общую программу обеспечения безопасности, включая вопросы эксплуатации и усовершенствования;
- — перечислять возможные угрозы информации и каналы ее утечки, результаты оценки опасностей и рекомендуемые защитные меры;
- — определять ответственных за внедрение и эксплуатацию всех средств защиты;
- — определять права и обязанности пользователей, причем таким способом, чтобы этот документ можно было использовать в суде при нарушении правил безопасности

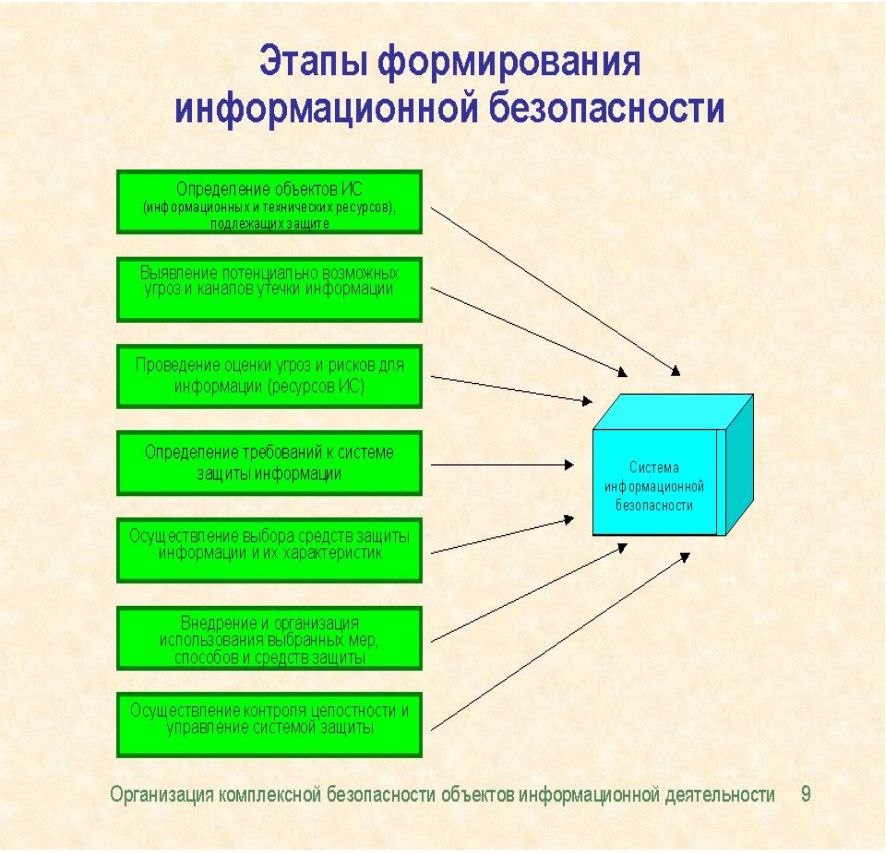
Прежде чем приступить к разработке документов, определяющих порядок ЗИ, нужно провести оценку угроз, определить информационные ресурсы, которые целесообразно защищать в первую очередь, и подумать, что необходимо для обеспечения их безопасности.

Правила должны основываться на здравом смысле. Целесообразно обратить внимание на следующие вопросы:

- — принадлежность информации; об информации обязан заботиться тот, кому она принадлежит;
- — определение важности информации; пока не определена значимость информации, не следует ожидать проявлений должного отношения к ней;
- — значение секретности; как пользователи хотели бы защищать секретность информации? Нужна ли она им вообще?

Если право на сохранение тайны будет признано в вашей организации, то может ли она выработать такие правила, которые обеспечивали бы права пользователей на защиту информации?

Состав нормативно-методического обеспечения



Нормативно-методическая документация должна содержать следующие вопросы защиты информации:

- — какие информационные ресурсы защищаются;
- — какие программы можно использовать на служебных компьютерах;
- — что происходит при обнаружении нелегальных программ или данных;
- — дисциплинарные взыскания и общие указания о проведении служебных расследований;
- — на кого распространяются правила;
- — кто разрабатывает общие указания;
- — точное описание полномочий и привилегий должностных лиц;
- — кто может предоставлять полномочия и привилегии;

- — порядок предоставления и лишения привилегий в области безопасности;
- — полнота и порядок отчетности о нарушениях безопасности и преступной деятельности;
- — особые обязанности руководства и служащих по обеспечению безопасности;
- — объяснение важности правил (пользователи, осознающие необходимость соблюдения правил, точнее их выполняют);
- — дата ввода в действие и даты пересмотра;
- — кто и каким образом ввел в действие эти правила.

План защиты информации может содержать следующие сведения:

- — назначение ИС;
- — перечень решаемых ИС задач;
- — конфигурация;
- — характеристики и размещение технических средств и программного обеспечения;
- — перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в ИС;
- — требования по обеспечению доступности, конфиденциальности, целостности различных категорий информации;
- — список пользователей и их полномочий по доступу к ресурсам системы;
- — цель защиты системы и пути обеспечения безопасности ИС и циркулирующей в ней информации;
- — перечень угроз безопасности ИС, от которых требуется защита, и наиболее вероятных путей нанесения ущерба;
- — основные требования к организации процесса функционирования ИС и мерам обеспечения безопасности обрабатываемой информации;
- — требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;
- — основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности ИС (особые обязанности должностных лиц ИС);

- — цель обеспечения непрерывности процесса функционирования ИС, своевременность восстановления ее работоспособности и чем она достигается;
- — перечень и классификация возможных кризисных ситуаций;
- — требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов. и т. п.);
- — обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы;
- — разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
- — определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
- — определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т. п.);
- — определение порядка разрешения споров в случае возникновения конфликтов.

Порядок разработки и внедрения документов

В статье 7 Закона РФ «О государственной тайне» заранее установлен состав сведений,

которые не могут быть засекречены, т. е. отнесены к государственной тайне.

- Не подлежат отнесению к государственной тайне и засекречиванию сведения:
- — о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствия, а также о стихийных бедствиях и их официальных прогнозах и последствиях;
- — о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- — о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- — о фактах нарушения прав и свобод человека и гражданина;
- — о размерах золотого запаса и государственных валютных резервах РФ;
- — о состоянии здоровья высших должностных лиц РФ;
- — о фактах нарушения законности органами государственной власти и их должностными лицами.

Полномочиями по отнесению сведений к государственной тайне обладают следующие органы государственной власти и должностные лица:

- 1. Палата Федерального собрания;
- 2. Президент Российской Федерации;
- 3. Правительство РФ;
- 4. Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий;
- 5. Органы судебной власти.

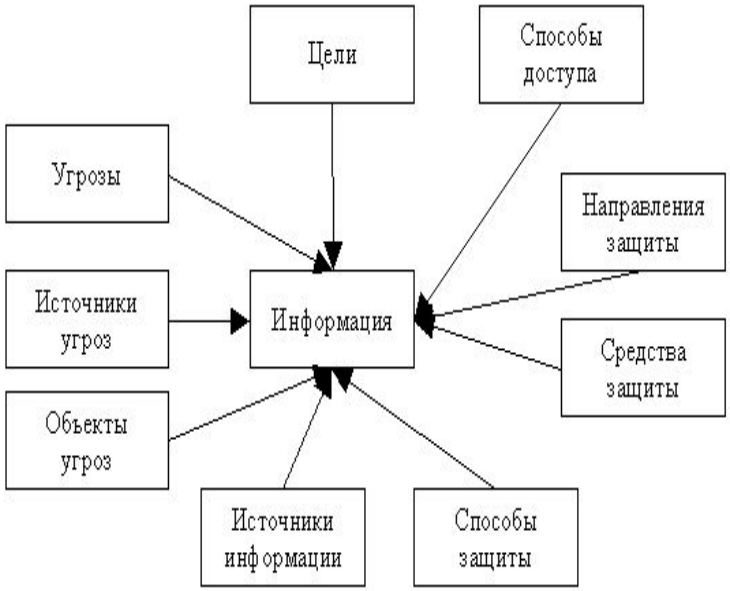
Основаниями для рассекречивания сведений являются:

- — взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;
- — изменение объективных обстоятельств, вследствие которых дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Экспертная комиссия

Для разработки перечня создается экспертная комиссия, в состав которой включаются компетентные специалисты, работающие со сведениями, составляющими государственную тайну.

В ходе подготовки проекта перечня экспертные комиссии в соответствии с принципами засекречивания сведений, установленными Законом Российской Федерации «О государственной тайне», проводят анализ всех видов деятельности соответствующих органов государственной власти, предприятий учреждений и организаций с целью определения сведений, распространение которых может нанести ущерб безопасности Российской Федерации. Обоснование необходимости отнесения сведений к государственной тайне с указанием соответствующей степени секретности осуществляется собственниками этих сведений и оформляется в виде предложений для включения в проект соответствующего перечня.



Утвержденные перечни в целях координации работ по защите государственной тайны направляются в Межведомственную комиссию.

После утверждения перечни доводятся до:

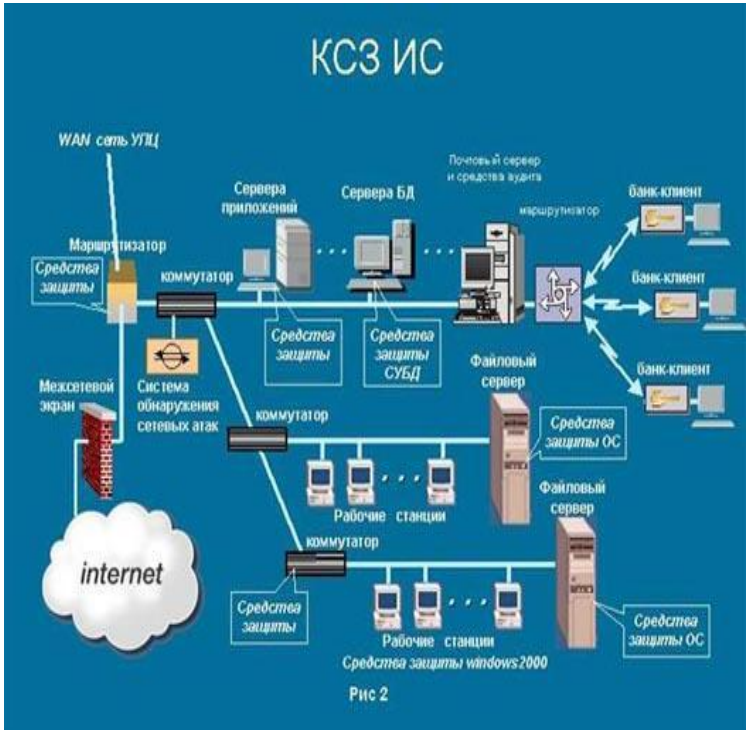
- — заинтересованных органов государственной власти в полном объеме либо в части, их касающейся;
- — предприятий, учреждений и организаций, действующих в сфере ведения органов государственной власти, в части, их касающейся, по решению должностного лица, утвердившего перечень;
- — предприятий, учреждений и организаций, участвующих в проведении совместных работ, в объеме, определенном заказчиком этих работ.

Серьезное значение для обеспечения безопасности информационных ресурсов приобретают документы предприятия,

регулирующие отношения с государством и с коллективом сотрудников на правовой основе.

К таким основополагающим документам можно отнести:

- — устав предприятия, закрепляющий условия обеспечения безопасности деятельности и защиты информации;
- — трудовые договоры с сотрудниками предприятия, содержащие требования по обеспечению защиты сведений, составляющих коммерческую тайну и др.;
- — правила внутреннего трудового распорядка рабочих и служащих;
- — должностные обязанности руководителей, специалистов и обслуживающего персонала.
- Эти документы играют важную роль в обеспечении безопасности предприятия.
- Для предприятия необходимо внести в устав следующие дополнения:
- — предприятие имеет право определять состав, объем и порядок защиты сведений, составляющих коммерческую тайну; требовать от своих сотрудников обеспечения ее сохранности;
- — обязано обеспечить сохранность коммерческой тайны;
- — состав и объем информации, являющейся конфиденциальной и составляющей коммерческую тайну, а также порядок защиты определяются руководителем предприятия;
- — имеет право не предоставлять информацию, содержащую коммерческую тайну;
- — руководителю предоставляется право возлагать обязанности, связанные с защитой информации, на сотрудников.



Внесение этих дополнений дает право администрации:

- — создавать организационные структуры по защите коммерческой тайны;
- — издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;
- — включать требования по защите коммерческой тайны в договора по всем видам деятельности;
- — требовать защиты интересов фирмы перед государственными и судебными органами;
- — распоряжаться информацией, являющейся собственностью, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства.

Отнесение к коммерческой тайне

В соответствии со ст. 139 ГК РФ и другими нормами федеральных

законов информация может составлять коммерческую тайну, если

она отвечает следующим требованиям (критерии правовой

охраны):

- — имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам;
- — не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;
- — к ней нет свободного доступа на законном основании;
- — обладатель информации принимает меры к охране ее конфиденциальности.

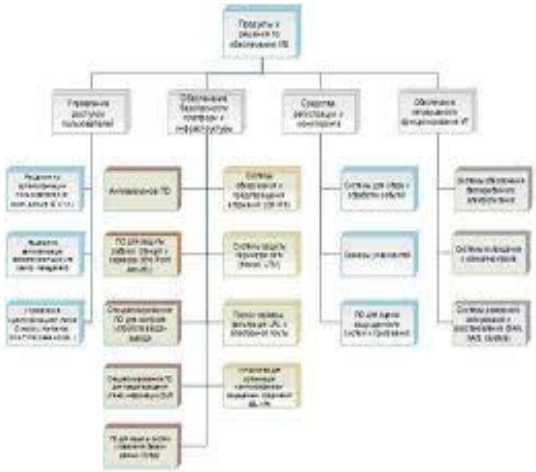
Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- 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.

Особые пункты трудового договора

В трудовой договор предприятия необходимо внести ряд пунктов соответствующего характера:

- 1. Работник обязан соблюдать конфиденциальности сведений, которые ему стали известны в процессе работы. В случае нарушения конфиденциальности работник несет материальную и административную ответственность в соответствии с действующим законодательством РФ и правилами внутреннего распорядка работодателя. Обязательства по соблюдению конфиденциальности остаются в силе и после прекращения срока действия настоящего договора в течение одного года;
- 2. Отдельную статью, связанную с конфиденциальностью, в которой бы содержалось следующее:
- 2.1. Под «Коммерческой тайной» понимаются носящие конфиденциальный характер сведения и их носители, полученные в рамках настоящего договора, и отвечающими следующим условиям:
- — сведения и их носители, указанные в «Перечне сведений, составляющих коммерческую тайну»;
- — сведения и их носители не являются общеизвестными или общедоступными из других источников;
- — сведения и их носители не передавались работодателем в распоряжение других лиц без обязательства, касающегося их конфиденциальности;
- 2.2. Под «Разглашением коммерческой тайны» понимаются умышленные или неосторожные действия работника, приведшие к преждевременному, не вызванному служебной необходимостью, открытому опубликованию сведений, составляющих коммерческую тайну, либо к утрате документов с такими сведениями или бесконтрольному использованию и распространению этих сведений.



Политика по сохранению коммерческой тайны реализуется путем максимального ограничения круга лиц, физической сохранности документов, содержащих такие сведения, внесения требований по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами и других мер по решению руководства.

- Защита и обработка конфиденциальных документов предусматривает:
- — порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;
- — систему допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую я тайну;
- — обеспечение сохранности документов на различных носителях с грифом конфиденциальности;
- — обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну;
- — принципы организации и проведения контроля за обеспечением режима при работе со сведениями, составляющим коммерческую тайну;
- — ответственность за разглашение сведений, утрату документов, содержащих коммерческую тайну.

Контрольные вопросы

1. Из чего состоит нормативно-методологическое обеспечение ИБ?
2. Какие документы регулируют деятельность по обеспечению ИБ в РФ?
3. Какие органы обладают полномочиями по отнесению сведений к государственной тайне?