|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Название документа** | **Описание** | **Доступ к документу** |
| **1** | **Доктрина информационной безопасности Российской Федерации** | 9 сентября 2000 года Президент России Владимир Путин утвердил «Доктрину информационной безопасности Российской Федерации».  Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.  Настоящая Доктрина служит основой для:   * формирования государственной политики в области обеспечения информационной безопасности Российской Федерации; * подготовки предложений по совершенствованию правового, методического, научно - технического и организационного обеспечения информационной безопасности Российской Федерации; * разработки целевых программ обеспечения информационной безопасности Российской Федерации.   Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере. | http://www.infotecs.ru/laws/security-doctrine/ |
| 2 | Стратегия развития информационного общества в РФ | Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти.  Увеличение добавленной стоимости в экономике происходит сегодня в значительной мере за счет интеллектуальной деятельности, повышения технологического уровня производства и распространения современных информационных и телекоммуникационных технологий.  Существующие хозяйственные системы интегрируются в экономику знаний. Переход от индустриального к постиндустриальному обществу существенно усиливает роль интеллектуальных факторов производства.  Международный опыт показывает, что высокие технологии, в том числе информационные и телекоммуникационные, уже стали локомотивом социально-экономического развития многих стран мира, а обеспечение гарантированного свободного доступа граждан к информации - одной из важнейших задач государств.  Динамика показателей развития информационной и телекоммуникационной инфраструктуры и высоких технологий в России не позволяет рассчитывать на существенные изменения в ближайшем будущем без совместных целенаправленных усилий органов государственной власти, бизнеса и гражданского общества. Необходимо уже в среднесрочной перспективе реализовать имеющийся культурный, образовательный и научно-технологический потенциал страны и обеспечить Российской Федерации достойное место среди лидеров глобального информационного общества.  В настоящей Стратегии закрепляются цель, задачи, принципы и основные направления государственной политики в области использования и развития информационных и телекоммуникационных технологий, науки, образования и культуры для продвижения страны по пути формирования и развития информационного общества. | http://www.infotecs.ru/laws/strategy/ |
| **3** | **Конституция РФ** | Законодательные акты, регулирующие вопросы информационной безопасности, так же как и законодательные акты во всех других областях, опираются на основной закон РФ – Конституцию РФ, принятую 12 декабря 1993 года.  Статья 23 Конституции РФ говорит:  «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.»  Статья 24:  «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободу, если иное не предусмотрено законом.»  Эти статьи являются законодательной основой защиты конфиденциальной информации. Каждый имеет право защищать свои личные данные, и никто не имеет права пытаться получить доступ к личным данным без согласия их владельца или решения суда.  Кроме того, часть 2 статьи 24 обязывает органы государственной власти и местного самоуправления обеспечить доступность информации, касающейся прав и свобод граждан.  Пункт 4 статьи 29 гарантирует каждому право “Свободно искать, получать, передавать, производить и распространять информацию любым законным способом”. Причём это право, также как и право на неприкосновенность частной жизни и право на ознакомление с документами, касающимися прав и свобод, не может быть ограничено даже в условиях чрезвычайного положения. В этом пункте говорится, что перечень сведений, составляющих государственную тайну, определяется федеральным законом.  В соответствии с другими статьями Конституции существует ряд сведений, которые не могут быть отнесены к государственной тайне и должны быть доступны гражданам.  В соответствии со статьёй 41 (часть 3), это сведение о “фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей”, а в соответствии со статьёй 42 – информация о состоянии окружающей среды.  Большое значение для практики использования информации, в том числе программ, имеет статья 44 Конституции, гарантирующая охрану законом интеллектуальной собственности. | http://starik2222.narod.ru/IB/48.htm |
| **4** | **Гражданский Кодекс РФ** | Вопросам информационной безопасности уделено внимание в Гражданском кодексе РФ, где фигурируют такие понятия, как банковская, коммерческая, служебная тайна. Согласно статье 139 ГК РФ информация составляет служебную или коммерческую тайну в случае, когда эта информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране её конфиденциальности. | http://starik2222.narod.ru/IB/48.htm |
| **5** | **Закон «Об информации, информатизации и защите информации»** | Основополагающим среди российских законов, посвящённых вопросам информационной безопасности, следует считать Федеральный закон РФ “Об информации, информатизации или защите информации”, принятый 25.01.95 года.  В нём даются основные определения и намечаются направления развития законодательства в данной области.  Согласно статье 1, этот закон регулирует отношения, возникающие при:  ·        Формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителям документированной информации.  ·        Создания и использования информационных технологий и средств их обеспечения.  ·        Защите информации и прав субъектов, участвующих в информационных процессах и информатизации.  При этом он не затрагивает отношений, регулируемых Законом РФ “Об авторском праве и смежных правах”.  Согласно статье 4 Закона, правовой режим информационных отношений определяется нормами, устанавливающими:  ·        Порядок документирования информации  ·        Право собственности на отдельные документы и массивы документов, в том числе в информационных системах  ·        Категорию информации по уровню доступа к ней  ·        Порядок правовой защиты информации  Статья 5, определяющая порядок документирования информации, в частности, является основой для использования электронной цифровой подписи. В статье, в частности говориться: “Юридическая сила документа, хранимого, обрабатываемого, передаваемого с помощью автоматизированной информационной системы, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдение установленного режима их использования» .  Статья 6 Закона определяет, кто является собственником информационных ресурсов. В частности, в ней указывается, что  “Физические и юридические лица являются собственниками тех документов (массивов документов), которые созданы за счет их средств, приобретены ими на законных основаниях, полученных в порядке дарения или наследования ”. Статья определяет права собственника информационных ресурсов, в том числе: назначать лица, осуществляющие хозяйственное ведение информационными ресурсами или оперативное управление ими; устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним, определять условия распоряжения документами при их копировании и распространении.  Статья 10 Закона определяет категории доступа к государственным информационным ресурсам. Статья говорит: «Информационным ресурсы РФ являются открытыми и общедоступными, за  исключением документированной информации, отнесенной законом к категориям ограниченного доступа, то есть информации, отнесенной к государственной тайне, и конфиденциальной информации».  В статье перечислены виды информации, доступ к которой не может быть ограничен.  Статья 11 Закона регламентирует использование персональных данных. В частности, указывается, что персональные данные относятся к категории конфиденциальной информации; что не допускается сбор, хранение и распространение информации о частной жизни и другой информации, нарушающей личную тайну; что персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации их прав и свобод.  Глава 5 Закона посвящена проблемам защиты информации и прав субъектов в области информационных процессов и информатизации.  Статья 20 Закона определяет, что целями защиты информации  Статья 21 Закона определяет, что защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб собственникам, владельцу, пользователю и иному лицу.  Статья 23 закона определяет цели и порядок защиты прав субъектов информационных отношений.  Статья 24 закона касается защиты права на доступ к информации. В частности, указывается, что отказ в доступе к открытой информации или предоставление пользователю заведомо недостоверной информации может быть обжалован в судебном порядке, а руководители и другие служащие органов государственной власти и организации, виновные в незаконным ограничении доступа к информации, несут ответственность в соответствии с уголовным и гражданским законодательством и законом «Об административных правонарушениях». | http://starik2222.narod.ru/IB/48.htm |
| **6** | **Уголовный кодекс РФ** | Конкретные наказания за нарушения информационной безопасности определены в уголовном кодексе РФ, глава 28 которого посвящена преступлениям в сфере компьютерной информации.  Статья 272 определяет наказания за неправомерный доступ к компьютерной информации: «Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если этот деяние повлекло уничтожение, блокирование модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети – называется штрафом в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от 2-х до 5-и месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2-х лет.  То же деяние, совершенное группой лиц по предварительному сговору или организованной группой лиц либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от 500 до 800 МРОТ или в размере заработной платы или иного дохода сужденного за период от 5 до 8 месяцев, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 3 до 6 месяцев, либо лишение свободы на срок до 5 лет.»  Статья 273 устанавливает наказание за создание, использование и распространение вредоносных программ для ЭВМ:  «Создание программ дли ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, бланкированию, модификации либо копированию информации, нарушению работы ЭВМ, систем ЭВМ или их сетей, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказывается лишением свободы на срок до 3-х лет со штрафом в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от 2-х до 5-и месяцев.  Те же действия, повлекли по неосторожности тяжкие последствия, наказываются лишением свободы от 3-х да 7-и лет»  Статья 274 устанавливает наказание за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сетей:  «Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сетей лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее  уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред -  наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5-и лет, либо обязательными работами на срок от 180 до 240 часов, либо ограничением свободы на срок до 2-х лет. То же действие, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до 4-х лет». | http://starik2222.narod.ru/IB/48.htm |
| **7** | **Гармонизированные критерии Европейских стран** (дата издания июнь 1991г) | Европейские Критерии рассматривают следующие составляющие информационной безопасности:   1. конфиденциальность, то есть защиту от несанкционированного получения информации; 2. целостность, то есть защиту от несанкционированного изменения информации; 3. доступность, то есть защиту от несанкционированного удержания информации и ресурсов.   В Критериях проводится различие между системами и продуктами. Система — это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт — это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. | http://thebard.narod.ru/kost/38.html |
| **8** | **Концепция защиты от несанкционированного доступа к информации** | Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД. Это — направление, связанное с СВТ, и направление, связанное с АС. Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.  В качестве главного средства защиты от НСД к информации в Концепции рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. | http://thebard.narod.ru/kost/38.html |
| **9** | [**Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 13.07.2015) "Об образовании в Российской Федерации" (с изм. и доп., вступ. в силу с 24.07.2015)**](http://www.consultant.ru/cons/document/cons_doc_LAW_140174/) | **Статья 29. Информационная открытость образовательной организации**  1. Образовательные организации формируют открытые и общедоступные информационные ресурсы, содержащие информацию об их деятельности, и обеспечивают доступ к таким ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте образовательной организации в сети "Интернет".  2. Образовательные организации обеспечивают открытость и доступность информации, копий:  3. Информация и документы, подлежат размещению на официальном сайте образовательной организации в сети "Интернет" и обновлению в течение десяти рабочих дней со дня их создания, получения или внесения в них соответствующих изменений. [Порядок](http://www.consultant.ru/cons/document/cons_doc_LAW_149242/#dst100010) размещения на официальном сайте образовательной организации в сети "Интернет" и обновления информации об образовательной организации, в том числе ее содержание и форма ее предоставления, устанавливается Правительством Российской Федерации. | http://www.consultant.ru/cons/document/cons\_doc\_LAW\_140174/ |
| **10** | Постановление Правительства Российской Федерации от 10 июля 2013 г. N 582 г. Москва"Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации" | 1. Правила определяют порядок размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" (далее соответственно - официальный сайт, сеть "Интернет") и обновления информации об образовательной организации, за исключением сведений, составляющих государственную и иную охраняемую законом тайну, в целях обеспечения открытости и доступности указанной информации. 2. Действие Правил не распространяется на образовательные организации, находящиеся в ведении Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации, Службы внешней разведки Российской Федерации, федерального органа исполнительной власти в области обеспечения безопасности и федеральных органов исполнительной власти, осуществляющих функции:  а) по выработке и реализации государственной политики и нормативно-правовому регулированию в области обороны;  б) по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции;  в) по контролю и надзору в сфере исполнения уголовных наказаний в отношении осужденных, содержанию лиц, подозреваемых или обвиняемых в совершении преступлений, и подсудимых, находящихся под стражей, их охране и конвоированию, контролю за поведением условно осужденных и осужденных, которым судом предоставлена отсрочка отбывания наказания, а также правоприменительные функции;  г) по выработке государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной охраны;  д) по выработке государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере оборота наркотических средств, психотропных веществ и их прекурсоров, а также в области противодействия их незаконному обороту. | http://www.rg.ru/2013/07/22/sait-site-dok.html |
| **11** | Постановление Правительства Российской Федерации N 1119 от 1 ноября 2012 года"Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" | 1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.  2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".  Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.  3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.  4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных". | http://securitypolicy.ru/index.php |
| **12** | Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» | Регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.  К информации, запрещенной для распространения среди детей, относится информация:  1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;  2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;  3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;  4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;  5) оправдывающая противоправное поведение;  6) содержащая нецензурную брань;  7) содержащая информацию порнографического характера;  8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего. | http://www.rg.ru/2010/12/31/deti-inform-dok.html |