

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«ЦЕНТР РАЗВИТИЯ РЕБЕНКА - ДЕТСКИЙ САД «СКАЗКА»

393760, Тамбовская область, г. Мичуринск, ул. Коммунистическая, д. 100  
(47545) 5-14-77 michskazka@yandex.ru / michskazka.68.edu.ru

**Доклад на тему:**  
**«Правовые основы информационной безопасности общества»**

старший воспитатель  
МБДОУ ЦРР - ДС «Сказка»  
Шарова И.С.

Мичуринск – Наукоград  
2017 год

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей информационные отношения, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих *законов, положений, постановлений и инструкций*, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности. В Конституции РФ гарантируется "тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений" (ст. 23, ч.2), а также "право свободно искать, получать, передавать, производить и распространять информацию любым законным способом" (ст. 29, ч.4). Кроме этого, Конституцией РФ "гарантируется свобода массовой информации" (ст. 29, ч.5), т. е. массовая информация должна быть доступна гражданам.

Концепция национальной безопасности РФ, введенная указом Президента РФ №24 в январе 2000 г., определяет важнейшие задачи обеспечения информационной безопасности Российской Федерации:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Для обеспечения прав граждан в сфере информационных технологий и решения задач информационной безопасности, сформулированных в Концепции национальной безопасности РФ, разработаны и продолжают разрабатываться и совершенствоваться нормативные документы в сфере информационных технологий.

### **Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации**

1. Закон Российской Федерации от 21 июля 1993 года №5485-1 "О государственной тайне" с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

- **государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной,

контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

- **носители сведений, составляющих государственную тайну**, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

- **система защиты государственной тайны** – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

- **доступ к сведениям, составляющим государственную тайну** – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

- **гриф секретности** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

- **средства защиты информации** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законом определено, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

**2. Закон РФ "Об информации, информатизации и защите информации"** от 20 февраля 1995 года №24-ФЗ – является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Основными задачами системы защиты информации, нашедшими отражение в Законе "Об информации, информатизации и защите информации", являются:

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п., вмешательства в информацию и информационные системы;

- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;

- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;
- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

В соответствии с законом:

- информационные ресурсы делятся на государственные и негосударственные (ст. 6, ч. 1);
- государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа (ст. 10, ч. 1);
- документированная информация с ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (ст. 10, ч. 2).

Закон определяет пять категорий государственных информационных ресурсов:

- открытая общедоступная информация во всех областях знаний и деятельности;
- информация с ограниченным доступом;
- информация, отнесенная к государственной тайне;
- конфиденциальная информация;
- персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом).

**Статья 22 Закона "Об информации, информатизации и защите информации"** определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации.

Следует отметить, что процесс законотворчества идет достаточно сложно. Если в вопросах защиты государственной тайны создана более или менее надежная законодательная система, то в вопросах защиты служебной, коммерческой и частной информации существует достаточно много противоречий и "нестыковок".

При разработке и использовании законодательных и других правовых и нормативных документов, а также при организации защиты информации важно правильно ориентироваться во всем блоке действующей законодательной базы в этой области.

Проблемы, связанные с правильной трактовкой и применением законодательства Российской Федерации, периодически возникают в практической работе по организации защиты информации от ее утечки по

техническим каналам, от несанкционированного доступа к информации и от воздействий на нее при обработке в технических средствах информатизации, а также в ходе контроля эффективности принимаемых мер защиты.

### **Ответственность за нарушения в сфере информационной безопасности**

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации.
- Кодекс Российской Федерации об административных правонарушениях.

В принятом в 1996 году **Уголовном кодексе Российской Федерации**, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

1. Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
2. Статья 140. Отказ в предоставлении гражданину информации.
3. Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
4. Статья 237. Соккрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.
5. Статья 283. Разглашение государственной тайны.
6. Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса "Преступления в сфере компьютерной информации". Глава 28 включает следующие статьи:

1. Статья 272. Неправомерный доступ к компьютерной информации.
  - a. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
  - b. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными

работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

2. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

а. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, – наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

б. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

3. Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

а. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети 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 пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

б. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

### **Административный уровень обеспечения информационной безопасности**

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности. Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Кроме этого, что немаловажно, именно на административном уровне определяются механизмы защиты, которые составляют третий уровень информационной безопасности – программно-технический.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Содержанием административного уровня являются следующие мероприятия:

1. Разработка политики безопасности.
2. Проведение анализа угроз и расчета рисков.

### **Разработка политики информационной безопасности**

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. С учетом этого рассмотрим следующее определение политики безопасности.

**Политика безопасности** – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Результатом разработки политики безопасности является комплексный документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Этот документ является основой практических мер по обеспечению безопасности и включает следующие группы сведений:

- основные положения информационной безопасности организации;
- область применения политики безопасности;
- цели и задачи обеспечения информационной безопасности организации;
- распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

Основные положения определяют важность обеспечения информационной безопасности, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.

В состав автоматизированной информационной системы входят следующие компоненты:

- **аппаратные средства** – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры), кабели, линии связи и т. д.;

- **программное обеспечение** – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

- **данные** – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

- **персонал** – обслуживающий персонал и пользователи.

Цели, задачи, критерии оценки информационной безопасности определяются функциональным назначением организации. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д.

Политика безопасности затрагивает всех субъектов информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить их права и обязанности, связанные с их непосредственной деятельностью.

С точки зрения обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):

- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- менеджер отдела;
- операторы;
- аудиторы.

В зависимости от размеров организации, степени развитости ее информационной системы, некоторые из перечисленных ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

**Специалист по информационной безопасности** (начальник службы безопасности, администратор по безопасности) играет основную роль в разработке и соблюдении политики безопасности предприятия. Он проводит расчет и перерасчет рисков, выявляет уязвимости системы безопасности по всем направлениям (аппаратные средства, программное обеспечение и т. д.).

**Владелец информации** – лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случаев именно владелец информации может определить ее ценность и конфиденциальность.

**Поставщики аппаратного и программного обеспечения** обычно являются сторонними лицами, которые несут ответственность за поддержание должного уровня информационной безопасности в поставляемых им продуктах.

**Администратор сети** – лицо, занимающееся обеспечением функционирования информационной сети организации, поддержанием сетевых сервисов, разграничением прав доступа к ресурсам сети на основании соответствующей политики безопасности.

**Менеджер отдела** является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за их выполнением на рабочих местах. Менеджеры должны доводить до подчиненных все аспекты политики безопасности, которые непосредственно их касаются.

**Операторы** обрабатывают информацию, поэтому должны знать класс конфиденциальности информации и какой ущерб будет нанесен организации при ее раскрытии.



**Аудиторы** – внешние специалисты по безопасности, нанимаемые организацией для периодической проверки функционирования всей системы безопасности организации.

Проблеме защиты информации уделяется особое внимание. На данный период в каждом учреждении имеется такой документ как «Политика безопасности» /имеется на сайте образовательной организации/.

В МБДОУ ЦРР - ДС «Сказка» разработан и утвержден приказом заведующего документ «Политика безопасности» (точное название *Политика в отношении обработки персональных данных* муниципального бюджетного дошкольного образовательного учреждения «Центр развития ребенка - детский сад «Сказка» г. Мичуринска Тамбовской области). Данный документ определяет принципы обработки персональных данных и общие подходы к реализации данных принципов обработки персональных данных. То есть наше учреждение является оператором, осуществляющим обработку персональных данных сотрудников, воспитанников и их родителей (законных представителей), а также физических лиц, состоящих в иных договорных отношениях с нашим учреждением. ДОУ занесено в РЕЕСТР операторов, осуществляющих обработку персональных данных на сайте РОСКОНАДЗРА.

Сейчас в нашем учреждении собираются, хранятся, обрабатываются, передаются в вышестоящие инстанции персональные данные сотрудников, детей. Поэтому сотрудники нашего ДОУ делают все, чтобы было соблюдено действующее законодательство в области защиты персональных данных.

Хочется отметить, что в настоящее время проблема защиты персональных данных является очень актуальной.

Для соблюдения требований закона «О персональных данных» (ПДн) ДОУ должно получает от сотрудников и родителей (законных представителей) каждого воспитанника, СОГЛАСИЕ НА ОБРАБОТКУ ПДн (на основании статьи 6, п. 1 ФЗ № 152- "О персональных данных").

МБДОУ ЦРР - ДС «Сказка» обрабатывает и защищает сведения о сотрудниках, детях и их родителях (законных представителях) на правовом основании.