Основы информационной безопасности

2020

Нормативные акты

- Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон № 152-ФЗ от27 июля 2006 г. «О персональных данных»;
- Федеральный закон № 436-ФЗ от 29 декабря 2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию».

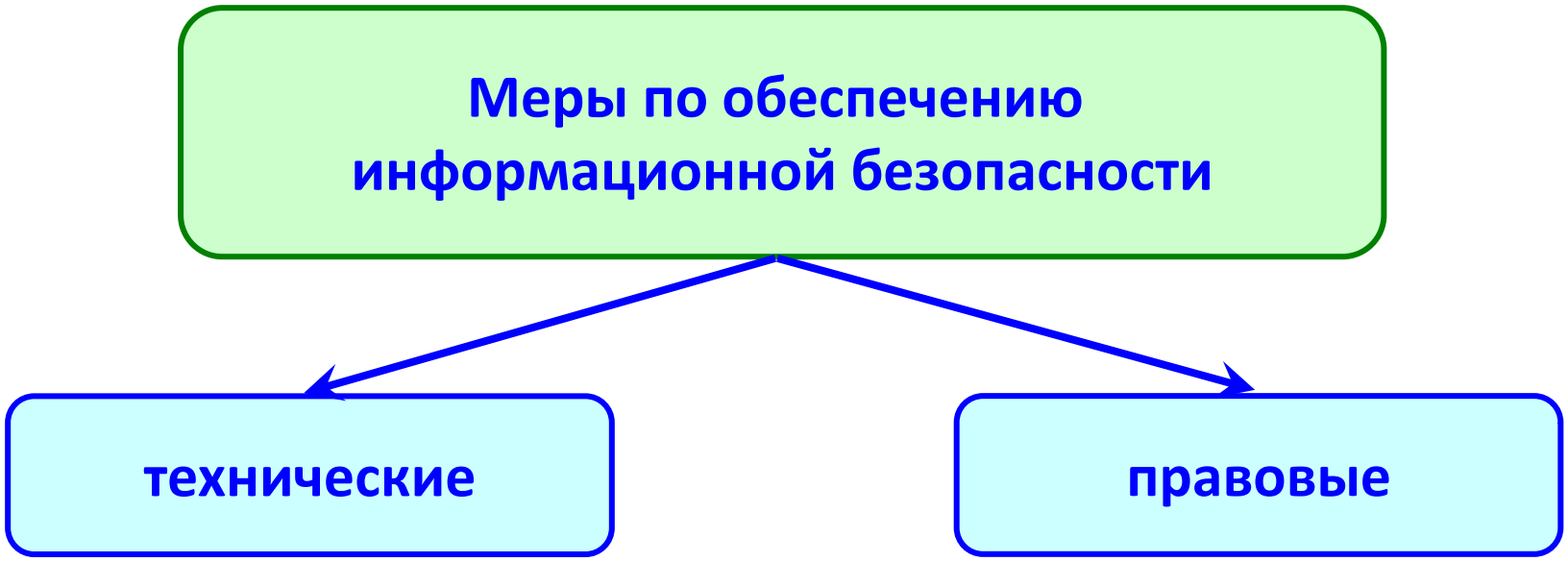
Основы информационной безопасности

- **Информационная безопасность** –

  состояние защищенности информационной среды.

- **Защита информации** – действия по предотвращению возможного повреждения или уничтожения информации, а также несанкционированного доступа к ней (но вместе с тем – обеспечение беспрепятственного доступа к информации).

Основы информационной безопасности



Аппаратные и программные средства и технологии защиты от вредоносных программ, внешних сетевых атак и пр. (в том числе антивирусные программы)

Совокупность нормативных и правовых актов, регулирующих вопросы защиты информации

Понятийный аппарат **Федерального закона №149-ФЗ**

- Понятие "***информация"*** определено как сведения (сообщения, данные) независимо от формы их представления.
- ***распространения информации*** - это действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.
- ***предоставления информации*** - это действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Понятийный аппарат **Федерального закона №149-ФЗ**

- ***Информационные технологии*** - это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
- ***Защита информации*** представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Понятийный аппарат **Федерального закона №149-ФЗ**

Две формы информации в зависимости от категории доступа к ней:

- **общедоступная информация**
- **информация ограниченного доступа**

Понятийный аппарат **Федерального закона №149-ФЗ**

- К **общедоступной информации** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен;

- **Информация ограниченного доступа**.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Информация, распространение которой в Российской Федерации ограничивается или запрещается

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

- Например: соответствии с ч. 2 ст. 5 Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию" ***к информации, запрещенной для распространения среди детей***, относится информация:

Информация, распространение которой в Российской Федерации ограничивается или запрещается

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- 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;

Информация, распространение которой в Российской Федерации ограничивается или запрещается

- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных названным Федеральным законом;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

Обладатель информации

- ***Обладатель информации*** – это лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

В законе перечислены субъекты, которые могут выступать в качестве обладателя информации, - это граждане (физические лица), юридические лица, Российская Федерация, субъекты РФ и муниципальное образование.

Обладатель информации

Обладатель информации имеет право:

- 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
- 3) передавать информацию другим лицам по договору или на ином установленном законом основании;
- 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

Обладатель информации

Обладатель информации при осуществлении своих прав **обязан**:

1) **соблюдать права и законные интересы иных лиц**

Обратите внимание!

Не допускаются осуществление гражданских прав исключительно с намерением причинить вред другому лицу, действия в обход закона с противоправной целью, а также иное заведомо недобросовестное осуществление гражданских прав (злоупотребление правом);

2**) принимать меры по защите информации**

Обладатель информации

Обладатель информации обязан обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

Обладатель информации

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

3) **ограничивать доступ к информации, если такая обязанность установлена федеральными законами.**

Понятийный аппарат **Федерального закона №149-ФЗ**

Информационная система - это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Виды информационных систем:

- **1) государственные информационные системы**, которые, в свою очередь делятся на федеральные информационные системы и региональные информационные системы.
- 2) **муниципальные информационные системы.** Данные информационные системы создаются на основании решений органов местного самоуправления

Понятийный аппарат **Федерального закона №149-ФЗ**

- 3) иные информационные системы.

Итак, с учетом нормы ч. 1 ст. 6 данного Закона, определяющей органы и лица, которые могут быть обладателями информации, - гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект РФ, муниципальное образование - можно говорить об информационных системах, созданных на основании решений гражданин и юридических лиц, т.е. о "частных" информационных системах.

Понятийный аппарат **Федерального закона №149-ФЗ**

- ***Оператором информационной системы*** является гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- Оператором информационной системы является либо собственник используемых для обработки, содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, либо лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Интернет: некоторые аспекты безопасного использования

Простейшие технологии безопасности:

- обновления,
- антивирус (авральная проверка компьютера, способы лечения блокированного вирусом компьютера, файлы, опасные по умолчанию),
- пароль,
- защита персональных данных,
- Фальшивый Яндекс и прочие ловушки.

Интернет: некоторые аспекты безопасного использования

Рис. 3

Интернет: некоторые аспекты безопасного использования

Электронные письма, переписка в социальных сетях

- ***Электронное сообщение*** - это информация, переданная или полученная пользователем информационно-телекоммуникационной сети (ст. 2 Закона об информации).
- ***Электронный документ*** - это информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, магнитных, оптических либо аналогичных средств, включая обмен информацией в электронной форме и электронную почту (абз. 2 п. 2 ст. 434 ГК РФ).

Информация в социальных сетях как повод для увольнения

- Допуская заключение договора путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору (абз. 1 п. 2 ст. 434 ГК РФ), законодатель ставит необходимое условие: 100%-ная возможность установить, что документ исходит именно от контрагента или его уполномоченного представителя.
- Как установить, что этот почтовый ящик принадлежит именно этому лицу?

Информация в социальных сетях как повод для увольнения

- В деловой практике применяют правило, которое может пригодиться и в житейских отношениях: если стороны договорились, что возможен обмен электронными сообщениями, то это должно быть прямо закреплено в договоре.

Например:

"Стороны признают юридическую силу электронных документов и переписки, направленных по адресам, указанным в разделе "Реквизиты сторон".

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

- Непринятие оператором мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами:

1.Отсутствие ответственного за организацию обработки персональных данных

2.Неиздание или неопубликование юридическим лицом документа, определяющий политику оператора в отношении обработки персональных данных;

3.Неиздание юридическим лицом локальных актов по вопросам обработки персональных данных.

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

4.Неосуществление внутреннего контроля/аудита соответствия обработки персональных данных требованиям законодательства Российских Федерации в области персональных данных.

5.Не ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и/или непроведение обучения указанных работников.

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

6.Отсутствие места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (П. 13 постановления правительства РФ от 15.09.2008 № 687)

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

ПРИМЕР УСТРАНЕНИЯ

ПРИКАЗ

об утверждении мест хранения материальных носителей персональных данных

В целях исполнения требований Федерального закона от 26.07.2006 № 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных в *(название)*

ПРИКАЗЫВАЮ:

1. Определить перечень мест хранения персональных данных обрабатываемых в *(название)*. (Приложение 1).
2. Контроль за исполнением настоящего приказа возложить *на ответственного за организацию обработки персональных данных Иванова В.В.*

_____ (руководитель организации) (подпись) _____ расшифровка подписи

«___»_____201_ г.

Приложение 1

ПЕРЕЧЕНЬ мест хранения персональных данных (ПДн), обрабатываемых в_____.

№ п/п	Подразделение	Место нахождения	Наименование документа, содержащего ПДн
1	Отдел кадров	Ул. Ленина 123, кабинет 1, шкаф/сейф	Личные дела сотрудников, трудовые книжки, приказы директора по личному составу.
2	Бухгалтерия	Ул. Ленина 123, кабинет 2	Индивидуальные сведения о трудовом стаже, заработке (вознаграждении), доходе и начисленных страховых взносах застрахованного лица; Расчетные (расчетно-платежные) ведомости; Листки нетрудоспособности
3	Библиотека	Ул. Ленина 123, кабинет 3	Учётные карточки и формуляры читателей библиотеки
4	…	…	…

Порядок работы с персональными данными (№ 152-ФЗ)

Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающий порядок обработки персональных данных работников, а так же об их правах и обязанностях в этой области.

Внимание! Ознакомление работников в электронном виде не в полной мере отвечает требованиям законодательства Российской Федерации.

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

Согласие в письменном форме на обработку персональных данных должно содержать:

1. ФИО, адрес субъекта персональных данных, номер основного документа, удостоверяющий его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2. ФИО, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющий его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных;

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

3. Наименование или ФИО и адрес оператора, получающего согласие субъекта персональных данных;
4. Цель обработки персональных данных;
5. Перечень персональных данных, на обработку которых дает согласие субъекта персональных данных;
6. Наименование или ФИО и адрес лица, осуществляющий обработку персональных данных по поручению оператора, если обработка поручена такому лицу;

Порядок работы с персональными данными (№ 152-ФЗ). Типичные нарушения

7. Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
8. Срок, в течение которого действует согласие субъекта персональных данных, а так же способ его отзыва, если иное не установлено федеральным законом;
9. Подпись субъекта персональных данных.

Биометрические персональные данные

- Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных

К биометрическим персональным данным относятся **физиологические данные:**

- дактилоскопические данные – отпечатки пальцев,
- радужная оболочка глаз,
- анализы ДНК,
- рост, вес и другие

Биометрические персональные данные

также иные физиологические или **биологические характеристики человека,** в том числе изображение человека:

- фотография
- видеозапись

Биометрические персональные данные

- В соответствии со ст. 152.1 Гражданского кодекса Российской Федерации обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) **допускаются только с согласия этого гражданина**.
- После смерти гражданина его изображение может использоваться только с согласия его законных представителей (супруги, дети, родители).

Биометрические персональные данные

БЕЗ СОГЛАСИЯ можно обрабатывать:

- 1) использование изображения осуществляется в **государственных, общественных или иных публичных интересах.**

Согласно п. 25 постановления Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. №16 к общественным интересам следует относить не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правовому государству и гражданскому обществу, общественной безопасности, окружающей среде.

Биометрические персональные данные

2) изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;

- Не требуется согласия гражданина, если изображение получено при съемке, которая проводится в местах, открытых для свободного посещения, например, открытых судебных заседаниях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях

НО: главным объектом на фото должно быть именно мероприятие, а не гражданин.

Биометрические персональные данные

- Изображение гражданина на фотографии, сделанной в публичном месте, не будет являться основным объектом использования, если в целом фотоснимок отображает информацию о проведенном публичном мероприятии, на котором он был сделан.
- Если же, как это часто бывает, фото сделано как бы в публичном месте, но превалирует все-таки личность (выделено и увеличено лицо, размыт фон, сама новость - об этом лице, а не о мероприятии), то согласие требуется.

Биометрические персональные данные

- 3) гражданин позировал **за плату**

Не требуется согласия и выплаты вознаграждения, если гражданин позировал за плату.

НО: тот факт, что человек сам разместил свое фото в Интернете, сам по себе не дает иным лицам права на свободное использование такого изображения без получения согласия изображенного лица.

Биометрические персональные данные

- при ведении **видеонаблюдения в** рабочих помещениях оператора с целью фиксации возможных действий противоправного характера согласно ст. 74 Трудового кодекса Российской Федерации **работники должны быть уведомлены об** изменении условий трудового договора по причинам, связанным с изменением организационных или технологических условий труда (введением видеонаблюдения), под роспись.

Биометрические персональные данные

- посетители публичных мест должны заранее предупреждаться их администрацией о возможной фото-, видеосъемке, соответствующими текстовыми и/или графическими предупреждениями.
- При соблюдении указанных условий **согласие субъектов** на проведение указанных мероприятии не требуется.

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

Информация, причиняющая вред здоровью и развитию детей – это информация, распространение которой среди детей запрещено или ограничено среди детей отдельных возрастных категорий.

Информационная безопасность детей - это состояние защищенности, при котором отсутствует риск , связанный с применением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Доступ детей к информации - это возможность получения и использования детьми свободно распространяемой информации.

Информационная продукция для детей - это информационная продукция , соответствующая по тематике , содержанию и художественному оформлению физическому, психическому, духовному, нравственному развитию детей.

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

Категории:

- 1) информационная продукция для детей, не достигших возраста 6 лет;
- 2) информационная продукция для детей, достигших возраста 6 лет;
- 3) информационная продукция для детей, достигших возраста 12 лет;
- 4) информационная продукция для детей, достигших возраста 16 лет;
- 5) информационная продукция, запрещенная для детей.

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

Реализация Концепции информационной безопасности детей должна обеспечить к 2020 году формирование в Российской Федерации поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве.

Должны быть создана ***новая медиасреда***, соответствующая следующим характеристикам:

- - наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
- - свободный доступ детей к историко-культурному наследию предшествующих поколений;
- - качественный рост уровня медиаграмотности детей;
- - увеличение числа детей, разделяющих ценности патриотизма;
- - гармонизация меж- и внутрипоколенческих отношений;
- - популяризация здорового образа жизни среди молодого поколения;
- - формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;
- - снижение уровня противоправного и преступного поведения среди детей;
- - формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента.

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

- 7 июня 2019 года Министерство просвещения РФ выпустило письмо N 04-474 «О методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 16 мая 2019 г.)».

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

Технологии организации системы ограничения обучающихся к негативной информации включают:

- 1. Контентную фильтрацию и ограничение доступа обучающихся к информации, включенной в Перечень видов информации, запрещенной к распространению посредством сети "Интернет", причиняющей вред здоровью и развитию детей, а также не соответствующей задачам образования - черный список;
- 2. Контентную фильтрацию и предоставление доступа обучающимся к сайтам в сети "Интернет", включенных в Реестр безопасных образовательных сайтов - белый список.

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

Формы организации системы ограничения обучающихся к негативной информации включают:

- 1. Использование на персональных устройствах, компьютере-сервере при использовании локальной сети и устройств для создания беспроводной сети (Wi-Fi) программного обеспечения, реализующего необходимый функционал;
- 2. Использование внешнего фильтрующего сервера, в том числе DNS-сервера и (или) прокси-сервера;
- 3. Получение услуг фильтрации через оператора связи либо специализированную организацию, обеспечивающую доступ в сеть "Интернет" для образовательной организации;

Особенности защиты детей от информации, причиняющей вред их здоровью и развитию (№ 436-ФЗ).

В зависимости от технологии СКФ (система контентной фильтрации) должна обеспечивать следующие ***основные функции***:

- 1. **Осуществлять в режиме реального времени анализ сайтов в сети "Интернет",** к которым обращаются пользователи, на предмет отсутствия на сайтах в сети "Интернет" информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- 2**. Пропускать, блокировать или модифицировать информацию** от сайта к пользователю в зависимости от результатов проверки;
- 3. **Автоматически передавать данные** во внешнюю систему о сайте, информация из которого удовлетворяет заданным правилам;
- 4. **Собирать статистику фильтрации**.