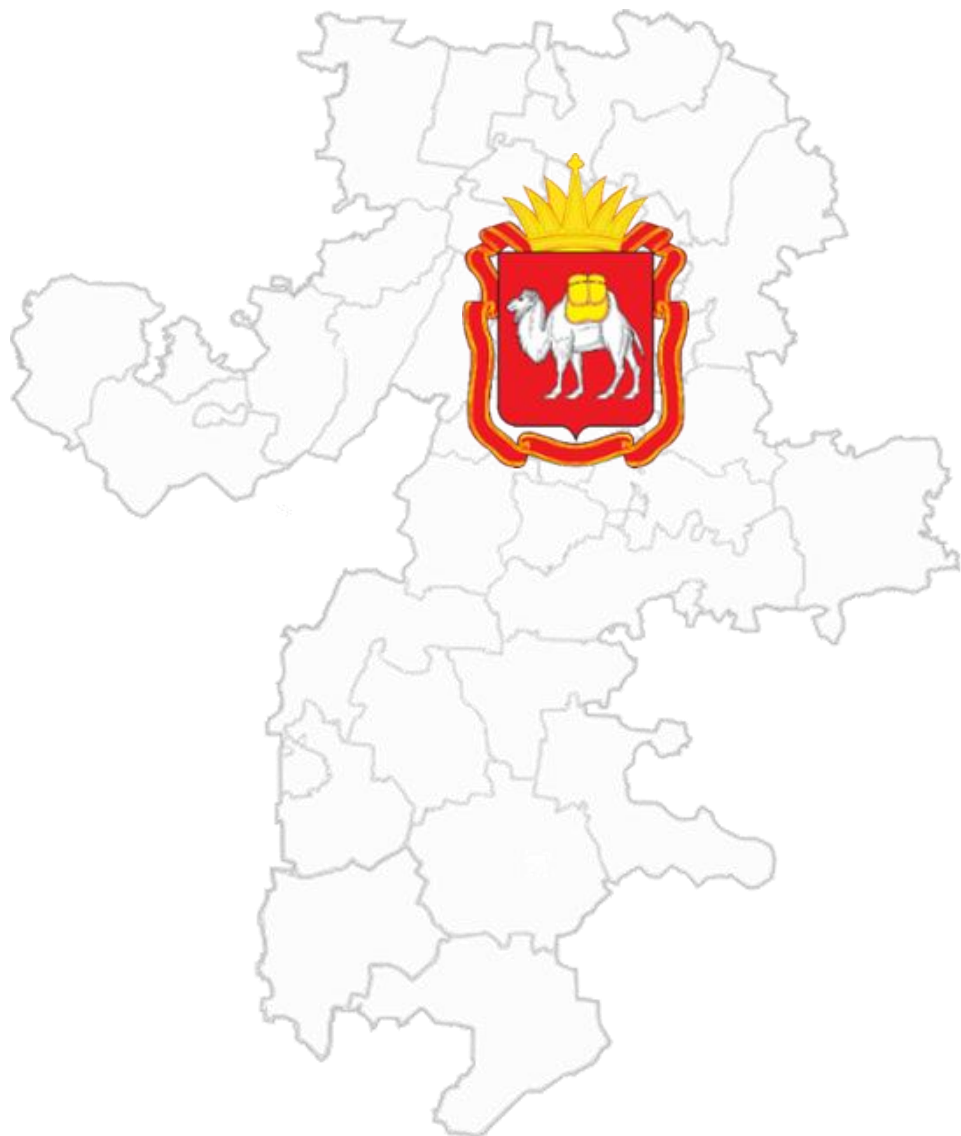




Обеспечение информационной безопасности образовательного процесса

Дмитриева Л.А., методист ОНМО ДПО
ГБУ ДПО «ЧИРО»



Нормативно-правовые основы информационной безопасности в образовательной организации



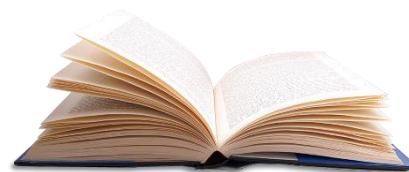
Нормативно-правовые основы информационной безопасности в образовательной организации



Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации».



Информация - сведения (сообщения, данные) независимо от формы их представления.





Статья 5 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации»:

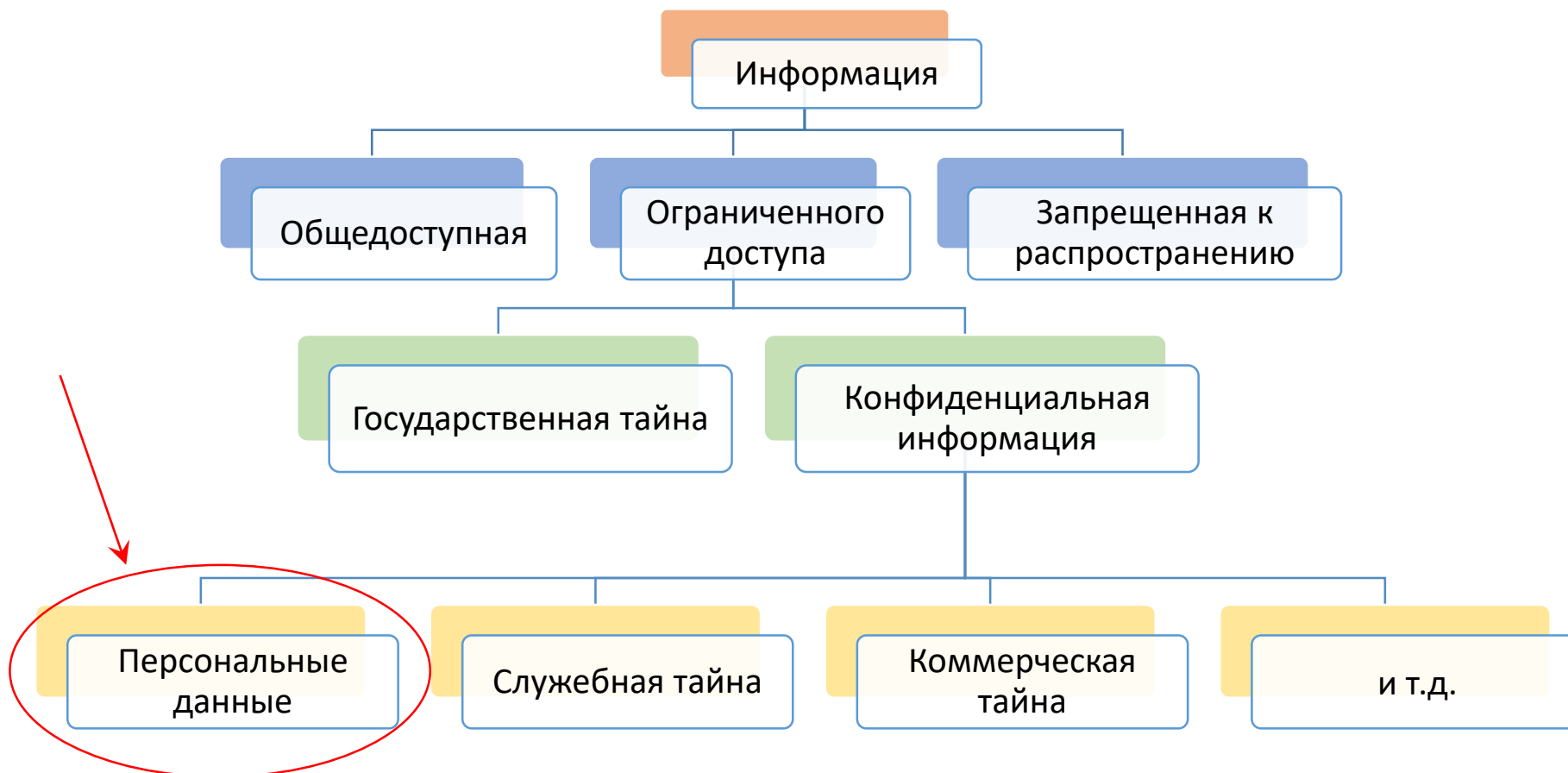
Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Нормативно-правовые основы информационной безопасности в образовательной организации



Классификация информации по категории доступа в РФ





Указ Президента РФ от 06 марта 1997 г. N188.

Перечень сведений конфиденциального характера:

1. Персональные данные
2. Сведения, составляющие тайну следствия
3. Служебная тайна
4. Сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская, тайна переписки, телефонных переговоров, почтовых отправлений и т.д.)
5. Коммерческая тайна
6. Сведения о сущности изобретения
7. Сведения, содержащиеся в личных делах осужденных



Статья 9 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации»:

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен.

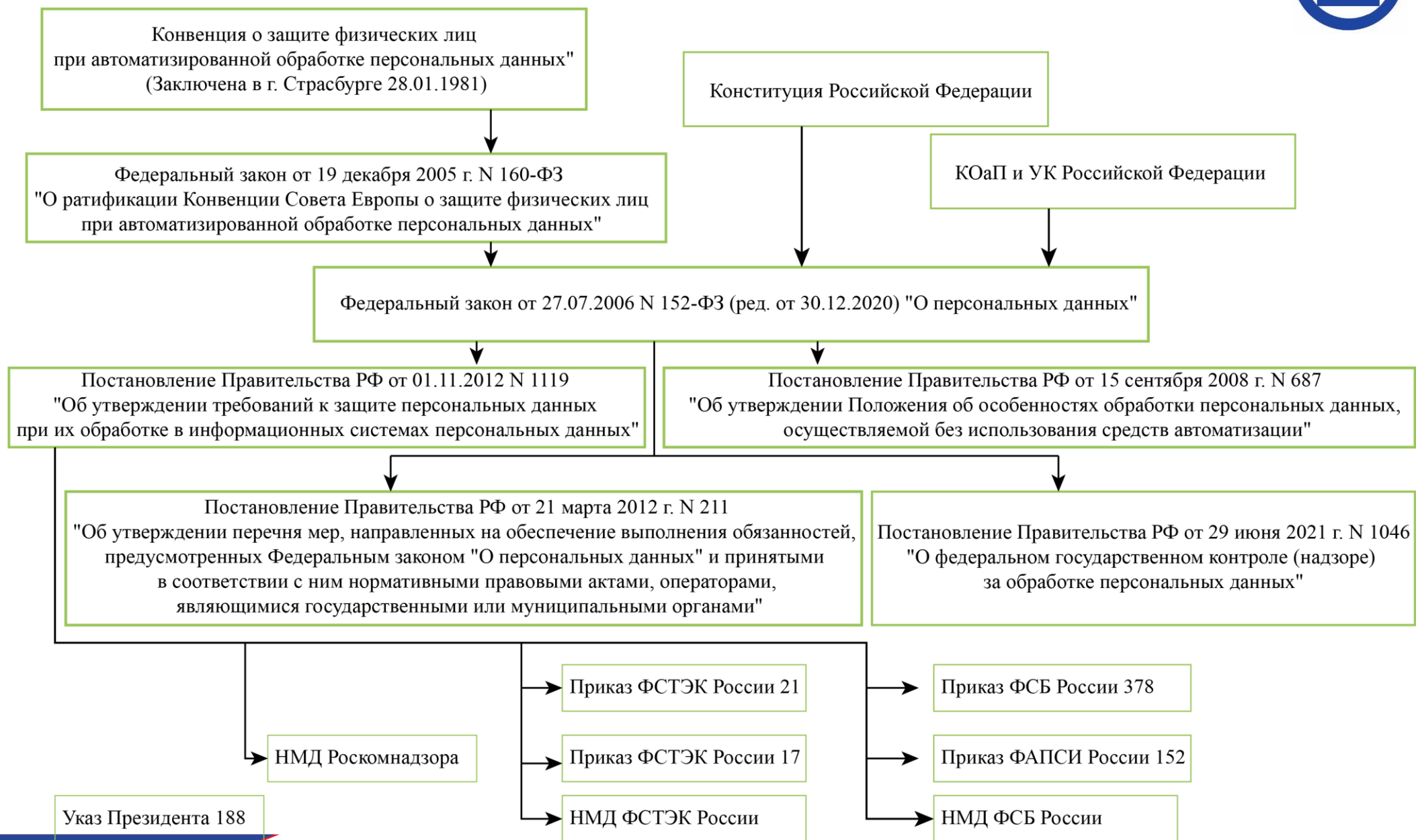
Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.



Персональные данные



Система «нормативных правовых актов» в области ПДн





- Федеральная служба по техническому и экспортному контролю — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.
- Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) — специальный орган^[1] Российской Федерации, с 24 декабря 1991 года по 11 марта 2003 года



Приказ ФСТЭК 21:

- Этот нормативный документ выступает в качестве дополнения к 152-ФЗ от 27.07.2006 г. Содержит рекомендации и требования по обеспечению технической защиты ПДн и предотвращению утечек данных. В частности, 21-й приказ ФСТЭК регламентирует:
- Порядок и принципы идентификации, аутентификации пользователей, допущенных к обработке ПДн;
- Особенности управления системой доступа к ПДн;
- Требования к программной среде, ограничения по использованию ПО;
- Обеспечение физической защиты ПК, на которых хранятся персональные сведения;
- Правила фиксации случаев инцидентов безопасности;
- Правила обеспечения антивирусной защиты;
- Методы учета случаев проникновения злоумышленников в закрытый информационный периметр;
- Порядок контроля, оценки защищенности ПДн.



- **Приказ ФСТЭК России № 17 от 11 февраля 2013 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».**
- **Кого касается**
- Обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы
- Операторов государственных информационных систем
- **Когда применяется**
- При обработке информации ограниченного доступа (не содержащей гостайну) или общедоступной информации в ГИС
- **Самое главное**
- Предприятия, обрабатывающие информацию ограниченного доступа в ГИС, обязаны разработать и внедрить систему защиты информации, отвечающую перечисленным в документе требованиям
- Информационная система должна быть аттестована по требованиям защиты информации организацией, у которой есть лицензия от ФСТЭК на деятельность по технической защите конфиденциальной информации



- **Приказ ФСБ России от 10 июля 2014 г. N 378**

"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

Нововведения



КоАП РФ ред. №441 от
09.03.2021 вступил в силу с
27.03.2021.

Ответственность за нарушение правил обработки ПДн (КоАП РФ ст. 13.11).



Правонарушения	Лица	Штрафы, тыс. руб		
		До 27.03.2021	Действующие	За повторное правонарушение с 27.03.2021
Обработка ПДн в случаях, не предусмотренных законом	Граждане	Предупреждение/ 1 - 3	2 - 6	4 - 12
	Должностные лица	Предупреждение/ 5 - 10	10 - 20	20 - 50
	Юридические лица	Предупреждение/ 30 - 50	60 - 100	100 - 300
Обработка ПДн без получения на то согласия субъекта	Граждане	Предупреждение/ 3 - 5	6 - 10	10 - 20
	Должностные лица	Предупреждение/ 10 - 20	20 - 40	40 - 100
	Юридические лица	Предупреждение/ 15 - 70	30 - 150	300 - 500
Не опубликование документа, определяющего политику оператора в отношении обработки ПДн	Граждане	Предупреждение/ 0,7 - 1	1,5 - 3	—
	Должностные лица	Предупреждение/ 3 - 6	6 - 12	—
	Юридические лица	Предупреждение/ 15 - 30	30 - 60	—

Ответственность за нарушение правил обработки ПДн (КоАП РФ ст. 13.11).



Правонарушения	Лица	Штрафы, тыс. руб		
		До 27.03.2021	Действующие	За повторное правонарушение с 27.03.2021
Не предоставление субъекту по запросу информации, касающейся обработки его ПДн	Граждане	Предупреждение/ 1 - 2	2 - 4	—
	Должностные лица	Предупреждение/ 4 - 6	8 - 12	—
	Юридические лица	Предупреждение/ 20 - 40	20 - 30	—
Невыполнение оператором требования субъекта об уничтожении, уточнении, блокировании ПДн	Граждане	Предупреждение/ 1 - 2	2 - 4	20 - 30
	Должностные лица	Предупреждение/ 4 - 10	8 - 20	30 - 50
	Юридические лица	Предупреждение/ 20 - 40	50 - 90	300 - 500
Невыполнение требований при сборе ПДн граждан РФ	Граждане	30 - 50	30 - 50	50 - 100
	Должностные лица	100 - 200	100 - 200	500 - 800
	Юридические лица	1 000 - 6 000	1 000 - 6 000	6 000 - 18 000
Невыполнение оператором требований при работе с ПДн без средств автоматизации правил обеспечения сохранности информации	Граждане	0,7 - 2	1 - 4	—
	Должностные лица	4 - 5	8 - 20	—
	Юридические лица	25 - 50	50 - 100	—



ФЗ №152 «О персональных данных» (ред. от 30.12.2020) вступил в силу с 01.03.2021.

С 01.03.2021 распространение только при наличии отдельного согласия по новой форме (приказ РКН от 24.02.2021 №18 – вступил в силу с 01.09.2021).

Требования по распространению (ст. 10.1 ФЗ №152 «О персональных данных») не применяются в случае обработки ПДн в целях выполнения возложенных законодательством РФ на ФОИВ, РОИВ, ОМСУ функций , полномочий и обязанностей.

Нормативно-правовые основы информационной безопасности в образовательной организации



Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) «О персональных данных».



Определяет:

- сферу действия, цели, понятия в области обработки ПДн;
- принципы и условия обработки ПДн;
- права субъектов, права и обязанности оператора ПДн;
- права и обязанности уполномоченного органа.



Статья 1 ФЗ №152 «О персональных данных»:

Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами.

Действие Федерального закона не распространяются на отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных.



Статья 2 ФЗ №152 «О персональных данных»:

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.



ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ





Основные понятия

Статья 3 ФЗ №152 «О персональных данных»:

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.



Основные понятия

Персональные данные – это :

- Паспортные данные;
- ФИО;
- Фотография;
- Дата и место рождения;
- Работа и должность;
- Номер телефона;
- Электронная почта;
- Персональный состав педагогических работников с указанием уровня образования, квалификации и опыта работы и т.д.



Основные понятия

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.



Основные понятия

Передача информации:

Доступ к информации — возможность получения информации и ее использования;

Предоставление информации — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Распространение информации — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.



Основные понятия

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Все ОО и МОУО являются операторами ПДн!



Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.



Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.



Принципы обработки ПДн

Ст. 5 №152 «О персональных данных».

1. Обработка ПДн должна осуществляться на законной и справедливой основе.
2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.
3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только ПДн, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.



Условия обработки ПДн

Ст. 6 №152 «О персональных данных».



Принципы и условия обработки ПДн

Глава 2 ст. 5 и 6 ФЗ №152 «О персональных данных»:

Обработка персональных данных должна осуществляться на законной и справедливой основе:

1. обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
2. с согласия на обработку ПДн.



Согласие на обработку ПДн

Статья 9 ФЗ №152 «О персональных данных»:

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных (специальные, общедоступные, иные) или с применением электронной подписи, что включает в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных



Согласие на обработку ПДн

- цель обработки персональных данных
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу *
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом
- подпись субъекта персональных данных.

*Особенности обработки персональных данных,
разрешенных субъектом персональных данных для
распространения*

Статья 10.1 ФЗ №152 «О персональных данных».

Требования к согласию на распространение – приказ
Роскомнадзора от 24.02.2021 №18.



Основы компьютерной безопасности при работе в сети интернет. (Кибергигиена)

Подавляющее большинство уязвимостей в системе безопасности создают сами люди. Поэтому все, что требуется, – это придерживаться элементарных правил осторожности в интернете:

1. Сертифицированное, лицензионное ПО для ЗИ
2. Регулярно делать резервные копии файлов.
3. Написание домена (https).
4. Не пишите пароли на стикерах и не сохраняйте в файлах на компьютере, не произносите их вслух при вводе.
5. Не «запоминайте» пароли в браузерах и не пользуйтесь программами автоматического ввода. Да, это удобно, но небезопасно: злоумышленники специально создают вирусы и программы для взлома такого ПО, чтобы похищать пароли.
6. Не вводить пароли и не передавать конфиденциальную информацию через общедоступные Wi-Fi.



Основы компьютерной безопасности при работе в сети интернет. (Кибергигиена)

Подавляющее большинство уязвимостей в системе безопасности создают сами люди. Поэтому все, что требуется, – это придерживаться элементарных правил осторожности в интернете:

7. Не пользуйтесь одним и тем же паролем для доступа к разным ресурсам. Если хакеры взломают один сайт, на котором вы использовали пароль, то все остальные ваши учетные записи с тем же паролем автоматически станут им доступны.
8. Не давайте доступ к своей учетной записи коллегам или подчиненным. Это грубое нарушение политики информационной безопасности. За все их действия, в том числе незаконные, будете отвечать лично вы.
9. Не открывать вложений в письмах, пришедших от незнакомых адресов.
10. Скачивайте приложения только из доверенных источников: с сайта производителя или из официальных магазинов приложений.
11. Надежные пароли.



Инструменты обеспечения информационной безопасности

Нет единого решения для всех организаций. Каждая из них должна сформировать свой уникальный набор инструментов для защиты информации с учетом своих особенностей.

Основы:

1. Организационно-распорядительная документация
2. Уведомление Роскомнадзора
3. Хранение ПДн
4. Передавать сведения в ФИС ФРДО (т.е. заполнять соответствующие ИС)
5. Соблюдение ФЗ-152.



454111, г. Челябинск, ул. Комсомольская, д. 20А
454087, г. Челябинск, ул. Блюхера, д. 91
454091, г. Челябинск, ул. Красноармейская, д. 88
454048, г. Челябинск, ул. Худякова, д. 20



info@chiro74.ru



8 (351) 217 30 89

МЫ В СОЦИАЛЬНЫХ СЕТЯХ



сайт ГБУ ДПО ЧИРО



Telegram-канал



Сообщество в ВКонтате



Сообщество в Одноклассниках