МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Государственное автономное образовательное учреждение
дополнительного профессионального образования
города Москвы
Московский центр развития кадрового потенциала образования
(ГАОУ ДПО МЦРКПО)

В.Р. Лещинер, к.п.н.

Методические рекомендации «Защита персональных данных обучающихся образовательных организаций»

Под общей редакцией Ю.В. Федоровой, к.п.н.

Москва, 2021

Защита персональных данных обучающихся образовательных организаций: методические рекомендации/ В.Р. Лещинер, к.п.н.; под общей редакцией Ю.В. Федоровой, к.п.н. – М.: Московский центра развития кадрового потенциала образования, 2021. 17 с.

В методических рекомендациях представлены нормативные документы, устанавливающие механизмы защиты персональных данных в информационных системах и компьютерных сетях и даны к ним пояснения, рассмотрены вопросы обеспечения защиты персональных данных обучающихся в условиях информационной открытости образовательных организаций, а также технические аспекты защиты персональных данных обучающихся.

Настоящие методические рекомендации предназначены для руководителей и педагогических работников образовательных организаций.

ОГЛАВЛЕНИЕ

НОРМАТИВНЫЕ ДОКУМЕНТЫ, УСТАНАВЛИВАЮЩИЕ МЕХАНИЗМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И КОМПЬЮТЕРНЫХ СЕТЯХ

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Основным нормативным документом, определяющим порядок работы с персональными данными в информационных системах и компьютерных сетях является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Согласно ст.3 этого закона «персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

Категории персональных данных

Согласно 152 ФЗ все персональные данные подразделяются на три категории:

Общие персональные данные: фамилия, имя отчество, дата и место рождения, паспортные данные (номера, даты и места выдачи документов, удостоверяющих личность, в т.ч. СНИЛС), домашний адрес, номера телефонов, сведения об образовании. В настоящее время очень многие сервисы привязаны к номеру мобильного телефона, поэтому он тоже относится к персональным данным.

Биометрические данные: информация о физиологических и биологических особенностях человека. Статья 11 152 ФЗ определяет их «Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность». Строго говоря, к биометрическим данным относится информация о росте и весе учащихся, но скорее всего, обработка этой информации обычным педагогическим работником не осуществляется. К биометрическим данным также относятся фотографические изображения, по которым можно определить биометрические параметры конкретного человека. Это фотоснимки лиц анфас, соответствующие по информативности фотографиям на документах, удостоверяющих личность.

Специальные категории персональных данных: информация о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. Персональные данные специальных категорий не должны обрабатываться в информационных системах, кроме специально определяемых законом случаев.

Обработка персональных данных

Согласно ст.3 152 ФЗ **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. Тем

самым любое действие с персональными данными является их обработкой и регулируется законом.

Одним из видов обработки данных является **распространение** персональных данных. Его регулирует статья 10.1 Закона «О персональных данных». Она введена Федеральным законом от 30.12.2020 N 519-ФЗ. Основное требование этой статьи – это то, что «Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения».

Так как учащиеся общеобразовательных организаций в подавляющем большинстве являются несовершеннолетними, согласие на обработку их персональных данных дается их родителями (законными представителями). Это согласие оформляется при зачислении учащегося в образовательную организацию и устанавливает конкретные ограничения этой обработки, в частности ограничения на распространение персональных данных. Педагоги общеобразовательных организаций должны хорошо представлять то, какие разрешения на обработку данных оформляются при приеме детей на обучение, равно как и понимать, что эти разрешения в любой момент могут быть отозваны, что потребует немедленное прекращение обработки персональных данных.

Трансграничная передача данных

Согласно ст.3 152 ФЗ **трансграничная передача персональных данных** - это «передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу». В связи с тем, что в виртуальном мире государственные границы провести трудно, надо понимать, что хранение данных на серверах информационных сервисов, находящихся за пределами Российской Федерации, является трансграничной передачей. Статья 12 152 ФЗ в ред. Федерального закона от 25.07.2011 N 261-ФЗ требует в общем случае оформления специального согласия субъекта персональных данных (родителей, законных представителей учащегося).

Федеральный закон "Об информации, информационных технологиях и о защите информации"

Другим важным нормативным документом в области охраны персональных данных является Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ. Он определяет общий порядок функционирования информационных систем в Российской Федерации и, в частности, порядок публикации материалов в сети Интернет. Этот закон содержит статью 7 «Общедоступная информация», в которой, в частности, говорится, что «Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации». Применительно к персональным данным обучающихся эта норма представляет собой требование получения согласия на публикацию персональных данных от субъектов данных (совершеннолетних обучающихся или родителей/законных представителей несовершеннолетних).

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ОТКРЫТОСТИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Обработка персональных данных обучающихся в образовательной организации

В общеобразовательной организации при осуществлении образовательной деятельности повседневно обрабатываются персональные данные обучающихся, относящиеся к различным категориям данных. Эти персональные данные включают:

- Общие персональные данные обучающихся, в т.ч. паспортные данные и данные о месте проживания, доступные широкому кругу работников общеобразовательной организации.
- Данные об успеваемости, текущих и итоговых оценках, прохождении учебного плана.
- Фотографии обучающихся, позволяющие установить их личность (относятся к биометрическим данным).
- Данные о здоровье (медицинская карта, карта прививок) – относятся к специальной категории персональных данных, должны обрабатываться отдельно лицом, имеющим допуск к медицинской документации (врачом, медсестрой, медрегистратором).
- В определенных случаях родители (законные представители) обучающегося представляют в образовательную организацию документы, содержащие сведения, необходимые

для предоставления учащемуся гарантий и компенсаций, установленных действующим законодательством: документы о составе семьи; документы о состоянии здоровья; документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством. Все эти документы должны быть категорированы в соответствии с 152 ФЗ и доступ к ним должен быть ограничен конкретным перечнем сотрудников образовательной организации.

Обязанности работников в отношении персональных данных учащихся

Работники, имеющие доступ к персональным данным учащегося, обязаны:

1. Не сообщать персональные данные обучающегося третьей стороне без письменного согласия одного из родителей (законного представителя), кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется.

2. Использовать персональные данные обучающегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя).

3. Обеспечить защиту персональных данных обучающегося от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации.

4. Ознакомить родителя или законного представителя с их правами и обязанностями в области защиты персональных данных, под роспись.

5. Соблюдать требование конфиденциальности персональных данных учащегося.

6. Исключать или исправлять по письменному требованию одного из родителей (законного представителя) обучающегося его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства.

7. Ограничивать персональные данные учащегося при передаче уполномоченным работникам правоохранительных органов или работникам органов управления образованием только той информацией, которая необходима для выполнения указанными лицами их функций.

8. Обеспечить совершеннолетнему обучающемуся или одному из родителей (законному представителю) несовершеннолетнего учащегося свободный доступ к персональным данным обучающегося, включая право на получение копий любой записи, содержащей персональные данные.

9. Предоставить по требованию одного из родителей (законного представителя) учащегося полную информацию о его персональных данных и обработке этих данных в образовательной организации.

Публикация персональных данных в сети Интернет

В соответствии со статьей 21 Федерального закона от 29.12.2012 N 273-ФЗ (в редакции от 30.04.2021) "Об образовании в Российской Федерации" «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"». Однако, указанная статья закона «Об образовании», устанавливая обязательный перечень размещаемой образовательной организацией информации, не предполагает публикации в сети персональных данных обучающихся (в отличие от персональных данных педагогических сотрудников и руководства образовательной организации). Поэтому недопустима публикация в сети в открытом доступе любых списков (классов, групп, приглашенных на мероприятие или собеседование, принятых на обучение и т.п.). Подобное информирование может быть осуществлено либо посредством электронной почты, либо с

использованием закрытых информационных систем, прежде всего электронного журнала/дневника.

Любая школа гордится успехами своих учеников и с удовольствием рассказывает о победах школьников на олимпиадах, спортивных соревнованиях, конкурсах и смотрах. Тем не менее, в соответствии с законодательством о защите персональных данных, такая информация, содержащая персональные данные, должна публиковаться только с письменного согласия субъекта персональных данных (в случае несовершеннолетнего обучающегося – родителя/законного представителя). В случае публикации биометрической фотографии, это должно быть специально отражено в согласии. В случае отзыва согласия на публикацию со стороны субъекта персональных данных, информация должна быть немедленно удалена с общедоступного информационного ресурса. В случае отсутствия согласия субъекта персональных данных на публикацию, образовательная организация может опубликовать обезличенную информацию, например указать только личное имя учащегося и опубликовать коллективное фото победившей команды без указания отдельных участников.

Также допустима публикация на сайте без получения согласия родителей (законных представителей) обучающихся репортажных фотографий общего плана, без указания персональных данных учащихся, запечатленных на фото.

ТЕХНИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Передача персональных данных обучающихся третьим лицам

Образовательная организация при осуществлении деятельности взаимодействует с большим количеством сторонних организаций. Это прежде всего органы управления образованием, а также органы Роспотребнадзора, соцзащиты, медицинские организации и т.д. Всем им периодически необходимо передавать какие-то персональные данные обучающихся. Так как согласие на передачу персональных данных родители обучающихся дают образовательной организации, то эти сторонние организации выступают в качестве третьих лиц в отношениях субъектов персональных данных с образовательной организацией. Образовательная организация должна включить организации, в которые регулярно передаются персональные данные, в текст согласия на обработку персональных данных, которое дается родителями учащегося при зачислении в образовательную организацию. В случае, если персональные данные надо передать организации, не включенной в этот перечень, следует получить согласие субъекта персональных данных на конкретную передачу данных.

При использовании электронных коммуникаций для передачи персональных данных, необходимо пользоваться специализированными информационными системами, такими

как портал госуслуг, электронный журнал/дневник, система ведомственного электронного документооборота и подобными. В частности, в каждой образовательной организации существует специальный компьютер с доступом к защищенному каналу связи с региональным центром обработки информации (РЦОИ) по которому передаются персональные данные участников государственной итоговой аттестации.

Следует избегать отправки персональных данных в открытом (на зашифрованном) виде по электронной почте, даже внутри корпоративной почтовой сети.

Специальные персональные данные (медицинская информация) должны обрабатываться и передаваться либо на бумажных носителях, либо внутри специализированных информационных систем, имеющих соответствующий уровень защиты и прошедших сертификацию (система электронных медкарт).

При использовании облачного хранения данных и документов общего доступа (мультипользовательских) для обработки персональных данных, надо быть уверенным, что не происходит трансграничной передачи данных. При использовании глобальных информационных сервисов (например, документов Google) такая трансграничная передача возможна, что создает риск нарушения образовательной организацией российского законодательства о защите персональных данных.

При передаче данных ответственность несет тот, кто данные передает, поэтому абсолютно недопустимо передавать любые персональные данные в ситуации, когда нет полной уверенности в том, что они попадут к надлежащему получателю. (Например, недопустимо отправлять персональные данные на электронный адрес на общедоступном почтовом сервисе (mail.ru, yandex.ru и т.п.), если нет абсолютной уверенности, что адрес администрируется надлежащим получателем).

Обеспечение контроля доступа к системам обработки персональных данных

Наиболее массовой системой обработки персональных данных в образовательной организации является электронный журнал/дневник. Педагогические работники обязаны предотвращать риски несанкционированного доступа к данным электронного журнала, соблюдая следующие правила:

- Использовать для входа в электронный журнал сильный пароль(не менее 8 символов, включая цифры и клавиатурные знаки) который периодически менять.

- Не использовать в качестве пароля легко подбираемые комбинаторно или с помощью социальной инженерии символы (подряд идущие буквы алфавита, цифры даты рождения и т.п.).

- Не хранить пароль для автозаполнения на общедоступном компьютере (на компьютере в учительской). Пользоваться автозаполнением паролей можно только на личном ноутбуке при условии непрерывного контроля над устройством со стороны владельца.

- На школьных стационарных компьютерах установить систему индивидуальных профилей для каждого пользователя с обязательным блокированием входа (необходимостью повторного ввода пароля) через непродолжительное время отсутствия активности.

- В случае использования для работы с информационной системой общедоступных компьютеров, включать режим «инкогнито», предполагающий уничтожение всех файлов cookie, очистку кэша и выход из всех аккаунтов при закрытии браузера.

- Входить в информационные системы, содержащие персональные данные, только на компьютерах с установленными актуальными антивирусными системами.

- В целях защиты персональных данных от компрометации не допускать заполнение электронного журнала неавторизованными лицами, прежде всего обучающимися.

Соблюдение этих правил, регулярное обновление паролей и антивирусных программ, очистка кэша и истории браузера позволит обеспечить надлежащий барьер несанкционированному доступу к персональным данным и конфиденциальной информации.