Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа № 127»

Приказ

«16» «марта» 2020 г. № 66а-осн.

г Барнаул

«Об организации работы по защите конфиденциальной информации и персональных данных»

В целях организации работы по защите конфиденциальной информации и персональных данных в МБОУ «СОШ №127» в соответствии с требованиями Федерального закона от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006г. № 152-ФЗ, и постановления Правительства РФ от 21.03.2012 № 211» Об утверждении перечня мер , направленных на обеспечение выполнения обязанностей . предусмотренных ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденного приказом Гостехкомиссии России от 30 августа 2002г. № 282, и других

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:

1.1. Перечни персональных данных, обрабатываемых в связи с реализацией трудовых отношений (Приложение 1 к данному Приказу).

1.2. Правила работы с обезличенными персональными данными (Приложение 2 к данному Приказу).

1.3. Организационные и технические мероприятия по технической защите конфиденциальной информации (Приложение 3 к данному Приказу).

1.4. Положение об обеспечении безопасности общедоступной информации в информационной системе (Приложение 4 к данному Приказу).

2. Контроль за исполнением Приказа возлагаю на себя.

Директор
МБОУ «СОШ №127» В.В.Сургаева.

Приложение №1
приказу № 66а-осн
от 16.03 2020г

Перечни персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций

I. ДОКУМЕНТЫ, В КОТОРЫХ СОДЕРЖАТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1.1 Документы, содержащие сведения, необходимые для заключения трудового договора с работником:

Паспорт или иной документ, удостоверяющий личность.
Документы об образовании, квалификации или наличии специальных знаний при поступлении на работу, требующих специальных знаний или специальной подготовки
Страховое свидетельство государственного пенсионного страхования.
Документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу.

1.2 Документы о составе семьи **работника, содержащие** сведения, необходимые **для предоставления работнику** гарантий **и компенсаций, установленных действующим** законодательством:

Свидетельство о браке.
Свидетельство о рождении ребенка и иные документы.

1.3Документы о **состоянии** здоровья **работника, в соответствии с которыми,** работник должен **пройти** предварительный **и периодические медицинские осмотры либо когда с наличием таких документов связано предоставление работнику** установленных **действующим** законодательством условий труда, каких-либо **гарантий и компенсаций:**
Медицинская книжка с медицинским заключением об отсутствии противопоказаний для занятия конкретным видом деятельности в образовательном учреждении.
Справка об инвалидности.
Справка о беременности и иные документы.

1.4 Документы, подтверждающие **право на дополнительные гарантии и** компенсации, предусмотренные действующим законодательством:

Справка о донорстве.

Документ, подтверждающий привлечение работника к исполнению государственных или общественных обязанностей и иные документы.
1.5 Документы о состоянии здоровья детей и других близких родственников, когда с **наличием таких документов связано предоставление работнику каких-либо** гарантий и **компенсаций.**

6. Иные документы, содержащие **сведения о персональных** данных работника:

Автобиография.
Свидетельство о постановке на налоговый учет.
Трудовой договор и приказ о приеме на работу. Трудовая
книжка.
Справка о доходах с предыдущего места работы. Приказы
о поощрениях и взысканиях.
Приказы об изменении условий трудового договора; Карточка унифицированной формы Т-2, утвержденная постановлением Госкомстата России от 05.01.2004 г. № 1 и иные документы.
Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;
- по истечении 75 лет срока их хранения;
- в других случаях, предусмотренных федеральными законами.

II. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

В состав персональных данных работника входят:

Имя, фамилия, отчество и документы, подтверждающие личность;

Пол, возраст, анатомические характеристики (рост, вес и др.) биометрические данные (изображение на фотографиях);

- Сведения об образование;
- Сведения о трудовом и общем стаже;
- Сведения о составе семьи;
- Сведения о воинском учете;
- Сведения о заработной плате сотрудника;
- Сведения о предыдущем месте работы;
- Сведения о социальных льготах; Наличие
- судимостей;
- Место жительства;
- Домашний телефон;
- Место работы или учебы членов семьи и родственников;
- Результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- Принадлежность лица к конкретной нации, этнической группе, расе;
- Привычки и увлечения (в том числе вредные), особенности взаимоотношений и общения с другими людьми (семейное положение и др.);
- Религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);

- финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);

Деловые и иные личные качества, которые носят оценочный характер;

Из указанного списка работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

III. ПОЛУЧЕНИЕ И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Источником информации обо всех персональных данных работника является непосредственно работник.

3.1 Персональные данные работника относятся к конфиденциальной информации. Для лица, получившего доступ к персональным данным, обязательным является требование не допускать распространение данной информации без согласия работника, а также при наличии иного законного основания. Требования при обработке персональных данных работника установлены статьей 86 Трудового кодекса РФ и не подлежат изменению и исключению.

3.2 Все персональные данные работника следует получать лично у работника. Информация о персональных данных работника предоставляется работником устно, либо путем заполнения различных анкет, опросных листов, которые хранятся в личном деле. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных (оформления запроса на прежнее место работы работника в целях выяснения его профессиональных качеств; запроса в учебное заведение о подлинности документа об образовании и т.п.) и последствиях отказа работника дать письменное согласие на их получение.

3.3 Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.4 Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудимым кодексом РФ или иными федеральными законами.

3.5 Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя, работника и третьих лиц.

3.6 Обработка персональных данных может осуществляться для статистических или иных научных и служебных целей при условии обязательного обезличивания персональных данных.

3.7 При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно с помощью электронных средств или в результате автоматизированной обработки таких данных.

Приложение №2

к приказу № 66а-осн

от 16.03. 2024

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ, ОБРАБАТЫВАЕМЫМИ В МБОУ «СОШ №127»

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №127» (далее – МБОУ «СОШ №127») разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных».

1.2. Настоящие Правила определяют порядок работы с обезличенными данными в МБОУ « СОШ №127».

2. Термины и определения

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

2.1.2. 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.

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

3. Условия обезличивания

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

3.2.1. Уменьшение перечня обрабатываемых сведений.

3.2.2. Замена части сведений идентификаторами.

3.2.3. Обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город).

3.2.4. Деление сведений на части и обработка в разных информационных системах.

3.2.5. Замена численных значений минимальным, средним или максимальным значением (например, нет необходимости обрабатывать сведения о возрасте каждого субъекта, достаточно обрабатывать данные о среднем возрасте по всей выборке или отдельным ее частям).

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в учреждении приведен в Приложении 1 к настоящим Правилам.

4. Порядок работы с обезличенными персональными данными

4.1. Работники МБОУ «СОШ №127», ответственные за обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

4.2. Директор МБОУ «СОШ №127», рассмотрев предложения, принимает решение о необходимости обезличивания персональных данных.

4.3. Работники МБОУ «СОШ №127», обслуживающие базы данных с персональными данными, совместно с ответственными за проведение мероприятий по обезличиванию обрабатываемых персональных данных в учреждении, осуществляют непосредственное обезличивание выбранным способом, не запрещенным действующим законодательством.

4.4. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

4.4.1. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение паролей, правил работы со съемными носителями, правил резервного копирования, правил доступа в помещения, где расположены элементы информационных систем, использование антивирусных программ.

4.4.2. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение: правил хранения бумажных носителей, правил доступа к помещениям, где они хранятся.

Приложение №1

Перечень

должностей МБОУ «СОШ №127», ответственных за проведение мероприятий

по обезличиванию обрабатываемых персональных данных

1. Директор школы
2. Зам. директора по УВР
3. Главный бухгалтер

Приложение №3
к приказу № 66а-ОД
от 16.03 2020 г

Организационные и технические мероприятия по технической защите конфиденциальной информации в МБОУ «СОШ №127»

1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются отдельными специалистами, назначаемыми руководителем учреждения для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии на право осуществления соответствующих работ.

2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

3. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

4. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя учреждения, эксплуатирующего объекты информатизации.

5. Техническая защита информации в защищаемых помещениях.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП (защищаемых помещениях) относятся:

5.5.1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России.

5.5.2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП, далее сотрудники, ответственные за безопасность информации.

5.5.3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

5.5.4. Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения.

5.5.5. Инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

6. Техническая защита информации в средствах вычислительной техники (СВТ) и автоматизированных системах (АС) от несанкционированного доступа в соответствии с требованиями руководящих документов Гостехкомиссии России должна обеспечиваться путем:

проведения классификации СВТ и АС;

выполнения необходимых организационных мер защиты;

установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД.

защита каналов связи, предназначенных для передачи конфиденциальной информации.

защиты информации от воздействия программ-закладок и компьютерных вирусов.

7. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

установки и применения средств антивирусной защиты информации;

обновления баз данных средств антивирусной защиты информации;

действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

7.1. Организация работ по антивирусной защите информации возлагается на руководителя учреждения и лиц, осуществляющих контроль за антивирусной защитой,

7.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;

периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

7.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

7.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

Входной антивирусный контроль всей информации поступающей с электронной почтой;

Входной антивирусный контроль всей поступающей информации из сети Internet;

Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

Периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

Обязательная антивирусная проверка используемых в работе внешних носителей информации;

Постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

Внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

Восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

7.5.Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

7.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом в подразделение по защите конфиденциальной информации или ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, поставить в известность подразделение информационно-технической службы органа власти по защите конфиденциальной информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями учреждения информационно-технической службы органа власти по защите конфиденциальной информации.

7.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

7.8. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

8. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на системного администратора

8.1. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.2 Формирование личных паролей пользователей осуществляется централизованно. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

8.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

8.4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

8.5. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.5.8.4 настоящей Инструкции.

8.7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности учреждения, периодический контроль – на специалиста по защите информации или ответственного сотрудника.