Землякова Ирина Викторовна

Подписан: Землякова Ирина Викторовна
DN: ИНН=233600703220, СНИЛС=00311267678, E=buxgalter101@mail.ru, C=RU, S=Краснодарский край, L=Краснодар, O=МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №. 101 ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА СТЕПАНА АНДРЕЕВИЧА НЕУСТРОЕВА, G=Ирина Викторовна, SN=Землякова, CN=Землякова Ирина Викторовна
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2022.11.11 16:29:53+03'00'
Foxit Reader Версия: 10.1.1

УТВЕРЖДАЮ
Директор МАОУ СОШ № 101
_____ И.В.Землякова

«___»_____2022г.

ПРАВИЛА
работы с обезличенными данными в муниципальном автономном общеобразовательном учреждении муниципального образования город Краснодар средней общеобразовательной школе № 101 имени Героя Советского Союза Степана Андреевича Неустроева

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила работ с обезличенными данными (далее Правила), устанавливают обязанности, права и порядок работы пользователей в информационных системах и на бумажных носителях муниципального автономного общеобразовательного учреждения муниципального образования город Краснодар средней общеобразовательной школы № 101 имени Героя Советского Союза Степана Андреевича Неустроева (МАОУ СОШ № 101), с обезличенными данными.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказ ФСТЭК от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Обезличивание персональных данных это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных и которые осуществляются в случаях, установленным законодательством Российской Федерации.

1.4. Ознакомление сотрудников МАОУ СОШ № 101 проводит администратор информационной безопасности информационных систем под подпись.

2. ПРИНЦИПЫ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможности их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

К свойствам обезличенных данных относятся:

полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);

структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);

релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме;

семантическая целостность (сохранение семантики персональных данных при их обезличивании);

применимость (возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание ПД);

анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

К характеристикам (свойствам) методов обезличивания ПД, определяющим возможность обеспечения заданных свойств обезличенных данных, относятся:

обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность);

вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию субъекта ПД);

возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием других операторов);

совместимость (возможность интеграции ПД, обезличенных различными методами);

параметрический объем (объем дополнительной информации, необходимой для реализации обезличивания и деобезличивания;

возможность оценки качества данных.

2.2 Требования к методам обезличивания подразделяются на:

Требования к свойствам, которыми должен обладать метод обезличивания;

Требования к свойствам, которыми должен обладать метод обезличивания.

3.ПРАВИЛА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ

Сотрудники обязаны:

Выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам.

Немедленно ставить в известность администратора ИСПД и руководителя подразделения в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также:

При подозрении на совершение попыток несанкционированного доступа к обезличенным данным, как в ИСПД, так и на бумажных носителях информации.

Использовать носители информации исключительно для выполнения своих служебных обязанностей.

Обеспечивать физическую безопасность носителей информации всеми разумными способами.

Извещать администраторов ИБ и ИСПД о фактах утраты (кражи) учтенных носителей информации.

При сдаче в ремонт ПК (ноутбука) в стороннюю организацию в обязательном порядке изымать жесткий магнитный диск с хранящимися на нём обезличенными данными.

Вход в помещение, где хранятся обезличенные данные, разрешен работникам, служебные обязанности которых предусматривают работу с данными документами. Доступ других лиц в данные помещения в случае служебной необходимости возможен только с разрешения директора МАОУ СОШ № 101.

Для хранения обезличенных данных на бумажных носителях организация обеспечивается необходимым количеством сейфов, в которых запрещается хранение предметов, не относящихся к данным документам.

Все замки сейфов должны иметь по два экземпляра ключей.

Вторые экземпляры ключей от них, а также от входных дверей помещений, где организовано хранение обезличенных данных, хранятся в сейфе

Лица, работающие с обезличенными данными на бумажных носителях информации, должны иметь на рабочем столе те документы, которые необходимы в данный момент, а все остальные должны находиться в сейфах или папках, на столе не должно быть посторонних бумаг. Работать с документами при открытых окнах разрешается в том случае, если на окнах имеются сетки, предотвращающие вылет документов из помещения и соблюдаются меры по защите от просмотра документов.

По окончании рабочего дня каждый исполнитель обязан проверить наличие находящихся у него документов и убрать их в сейфы. Сейфы закрыть и сдать под охрану.

Сотрудникам категорически ЗАПРЕЩАЕТСЯ:

Хранить и обрабатывать личную информацию на ПК (ноутбуке), где обрабатываются обезличенные данные.

Оставлять без присмотра включенную ПК (ноутбук), не активизировав средства защиты от НСД.

Оставлять без присмотра документы с обезличенными данными на рабочем месте, выходя из кабинета.

Оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа.

Использование для хранения и обработки обезличенных данных машинных носителей информации, не поставленных на учет в установленном порядке.

Использовать носители информации в личных целях.

Передавать носители информации другим лицам (за исключением администраторов ИБ и администраторов ИСПД).

Хранить съемные носители с обезличенными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

Выносить съемные носители с обезличенными данными из служебных помещений для работы с ними на дому и т. д.

4.ПОРЯДОК ПЕРЕСМОТРА ПРАВИЛ

Правила подлежат полному пересмотру в следующих случаях:

- при изменении перечня решаемых задач, организационных мер, состава технических и программных средств ИСПД МАОУ СОШ № 101, приводящих к существенным изменениям технологии обработки информации.

Правила подлежат частичному пересмотру в остальных случаях.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных, совместно с директором МАОУ СОШ № 101 с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПД МАОУ СОШ № 101.

Вносимые изменения не должны противоречить другим положениям Правил.

5.ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ

Ответственным за постоянный контроль выполнения требований данных Правил является администратор информационной безопасности информационных систем МАОУ СОШ № 101.

ПРИЛОЖЕНИЕ 1 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Лист ознакомления с «Правилами работ с обезличенными данными»

№ п/п	Ф.И.О. сотрудника	Дата ознакомления	Подпись сотрудника в ознакомлении

Лист ознакомления с «Правилами работ с обезличенными данными»

№ п/п	Ф.И.О. сотрудника	Дата ознакомления	Подпись сотрудника в ознакомлении

Лист ознакомления с «Правилами работ с обезличенными данными»

№ п/п	Ф.И.О. сотрудника	Дата ознакомления	Подпись сотрудника в ознакомлении