

Муниципальное общеобразовательное учреждение
«Средняя общеобразовательная школа №3 города Буденновска Буденновского района»
356800 г. Буденновск Ставропольского края ул.Кумская,47
тел/факс: 8 (86559) 2-42-56
E-mail: busoch3@mail.ru
ОКПО 50229630, ОГРН 1022603224665
ИНН/КПП 2624022016/262401001

ПРИКАЗ

от 13.10.2021 года

№ 347 ОД

Об утверждении инструкции

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», приказа ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и прочих нормативных документов по защите информации

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие инструкцию администратора информационных систем персональных данных (приложение 1).
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор школы

С приказом ознакомлен(а):

1.И.В. Щербак



М.Ю. Мурдугова

ИНСТРУКЦИЯ

администратора информационных систем персональных данных

ГБУ ДО «КЦЭТК»

1. Термины и определения

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

1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбой программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. 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.

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

1.5. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция определяет функции, обязанности и права администратора информационных систем персональных данных (далее – администратор ИСПДн).

2.2. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее – ПДн), не исключает обязательного выполнения их требований.

2.3. Администратор ИСПДн назначается приказом директора учреждения.

2.4. На время отсутствия (болезнь, отпуск, пр.) администратора ИСПДн, его обязанности возлагаются на работника, назначенного и допущенного в установленном

порядке.

3. Функциональные обязанности

3.1. Администратор ИСПДн выполняет следующие функции:

3.1.1. Управляет параметрами ИСПДн:

- управляет заведением и удалением учетных записей пользователей;
- управляет полномочиями пользователей;
- поддерживает правила разграничения доступа;
- управляет параметрами настройки программного обеспечения;
- управляет учетными записями пользователей программных средств обработки ПДн;
- оказывает помощь в смене и восстановлению паролей;
- управляет установкой обновлений программного обеспечения;
- регистрирует события в ИСПДн, связанные с защитой ПДн (события безопасности);
- поддерживает конфигурацию ИСПДн (структуру ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;
- восстанавливает работоспособность программного обеспечения и технических средств ИСПДн.

3.1.2. Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности ПДн:

- отказы в обслуживании;
- сбои (перезагрузки) в работе технических средств и программного обеспечения;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору ПДн;
- иные события, приводящие к возникновению инцидентов.

3.1.3. Своевременно информирует ответственного за обеспечение безопасности ПДн в ИСПДн, о возникновении инцидентов в ИСПДн;

3.1.4. Принимает меры по устранению инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- по устранению последствий нарушения правил разграничения доступа, несанкционированного доступа к ПДн, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.

3.1.5. Ведет учет пользователей ИСПДн;

3.1.6. Принимает участие в деятельности по:

- подготовке, пересмотру, уточнению локальных актов по защите ПДн;
- аттестации объектов информатизации.

4. Права

4.1. Администратор ИСПДн имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований инструкций по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования системы защиты ПДн;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

5.1. Администратору ИСПДн категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных (личных) целях;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

5.2. На Администратора ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования ИСПДн.

5.3. Администратор несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

6.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора учреждения.