Приложение
к приказу

УТВЕРЖДАЮ
Рохо-Фернандес Т.Л.

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Данная Инструкция является руководящим документом ответственного за обеспечение безопасности персональных данных в МБОУ СОШ №2 г.Томари Сахалинской области (далее – Оператор).

Требования ответственного за обеспечение безопасности персональных данных, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками Оператора.

Ответственный за обеспечение безопасности персональных данных назначается приказом руководителя Организации из числа руководителей структурных подразделений, входящих в информационно-технологическую службу Организации.

Ответственный за обеспечение безопасности персональных данных подчиняется руководителю Организации, получает указания непосредственно от него и подотчетен только руководителю Организации.

Ответственный за обеспечение безопасности персональных данных в своей деятельности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- настоящей Инструкцией.

2. ОБЯЗАННОСТИ

В обязанности ответственного за обеспечение безопасности персональных данных входит:

— обеспечение непрерывного функционирования системы защиты персональных данных (далее – СЗПДн) в целом, ее программных и технических компонентов;

— настройка прав доступа сотрудников к персональным данным (далее – ПДн) и средствам их обработки согласно требованиям по информационной безопасности ПДн Оператора;

— разработка для пользователей информационных систем персональных данных инструкций по работе со средствами защиты информации;

— ведение журналов учета, входящих в состав организационно-распорядительной документации у Оператора;

— предоставление экспертных консультаций и рекомендаций сотрудникам, участвующим в обработке и обеспечении безопасности персональных данных (далее – ПДн) у Оператора, по вопросам использования средств защиты информации;

— хранение эталонного программного обеспечения средств защиты информации;

— ведение учета носителей ПДн и обеспечение их безопасного уничтожения согласно принятым у Оператора Регламентом по учёту, хранению и уничтожению носителей персональных данных;

— контроль обслуживания, настройки и ремонта средств обработки и средств защиты ПДн;

— сопровождение и контроль сторонних организаций (подрядчиков) в случае привлечения их для обслуживания, настройки и ремонта средств обработки и средств защиты ПДн;

— настройка конфигураций средств защиты информации, используемых для обеспечения безопасности ПДн;

— предоставление необходимой информации при проведении проверок уполномоченными органами и при проведении контрольных мероприятий по защите ПДн;

— реагирование на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн;

— участие во взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

— информирование в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных;

— уведомление уполномоченного органа по защите прав субъектов персональных данных о факте неправомерной или случайной передаче (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;

— в случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных;

3. ДОЛЖЕН ЗНАТЬ

Ответственный за обеспечение безопасности персональных данных должен знать:

- нормативно-правовые акты, регламентирующие вопросы обработки и защиты персональных данных;

- локальные нормативные акты и организационно-распорядительные документы по вопросам обработки и защиты персональных данных;

- особенности обработки и защиты персональных данных в Организации;

4. ПРАВА

Ответственный за обеспечение безопасности персональных данных имеет право:

— осуществлять подготовку предложений по внесению изменений в организационно-распорядительную документацию на СЗПДн Оператора;

— запрашивать у сотрудников, участвующих в обработке и обеспечении безопасности ПДн, информации и документов, необходимых для выполнения своих функциональных обязанностей;

— вносить предложения руководителю Организации в внесении изменений в локально-нормативные акты и организационно-распорядительную документацию Оператора;

— запрашивать у работников, участвующих в обработке и обеспечении безопасности персональных данных, информацию и документы, необходимые для выполнения его функциональных обязанностей;

— участвовать в рассмотрении проектов решений по вопросам своей компетенции;

5. ОТВЕТСТВЕННОСТЬ

Сотрудник, выполняющий функции ответственного за обеспечение безопасности персональных данных, несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

За несоблюдение требований федерального законодательства о персональных данных предусмотрена гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством Российской Федерации ответственность.

В случае нарушения установленного федеральным законодательством порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) предусмотрены административные штрафы, определенные действующим законодательством РФ.

Руководитель Организации вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

С инструкцией ознакомлен:

_____ _____