РЕГИОНАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ И КОНТРОЛЮ В СФЕРЕ ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

07.10.2019 № 3

г. Ростов-на-Дону

Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых Региональной службой по надзору и контролю в сфере образования Ростовской области при осуществлении переданных полномочий Российской Федерации в сфере образования

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Региональная служба по надзору и контролю в сфере образования Ростовской области постановляет:

1. Утвердить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых Региональной службой по надзору и контролю в сфере образования Ростовской области при осуществлении переданных полномочий Российской Федерации в сфере образования, согласно приложению.
2. Настоящее постановление вступает в силу со дня его официального опубликования.
3. Контроль за выполнением настоящего постановления оставляю за собой.

Руководитель Региональной службы Н.В. Толстик

Постановление подготовлено
сектором информационно-
программного обеспечения

Приложение
к постановлению
Региональной службы
по надзору и контролю
в сфере образования
Ростовской области
от 07.10.2019 № 3

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых Региональной службой по надзору и контролю в сфере образования Ростовской области при осуществлении переданных полномочий Российской Федерации в сфере образования

1. Угроза длительного удержания вычислительных ресурсов пользователя.
2. Угроза доступа/перехвата/изменения HTTP cookies.
3. Угроза использования слабостей протоколов сетевого/локального обмена данными.
4. Угроза определения топологии вычислительной сети.
5. Угроза подмены содержимого сетевых ресурсов.
6. Угроза «кражи» учетной записи доступа к сетевым сервисам.
7. Угроза неправомерного шифрования информации.
8. Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты.
9. Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.