

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 02D4A4B20049B10B9545700C42FFB251B7
Владелец ЧОУ ДПО "ИППК"



Частное образовательное учреждение
дополнительного профессионального образования
«Институт переподготовки и повышения квалификации»
ЧОУ ДПО «ИППК»

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(программа повышения квалификации)

«Информационная безопасность в образовательной организации»

г.Новочеркасск
2024 г.

Аннотация к рабочей программе.

Цель обучения по программе: овладение слушателями актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний, развитие практических навыков по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации, защиту воспитанников образовательных учреждений от негативной и запрещенной информации в Интернете, организационную и методическую поддержку педагогов.

Поставленная цель достигается решением следующих задач:

- изучением правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;
- изучением методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;
- практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- изучением методов и процедур обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду;
- практической отработкой способов и порядка проведения работ по обеспечению эффективной работы системы контент-фильтрации;
- практической отработкой способов и порядка использования в образовательном процессе цифровых образовательных ресурсов (ЦОР);
- практической отработкой способов и порядка обеспечения информационной безопасности локальной сети образовательного учреждения.

Категория слушателей: специалисты органов государственной власти, местного самоуправления, образовательных организаций и учреждений всех видов форм и собственности.

Режим занятий: 36 часов самостоятельной работы в неделю.

В результате изучения курса слушатели должны:

быть ознакомлены:

с нормативными правовыми и организационными основами защиты информации и обеспечения безопасности персональных данных в Российской Федерации;

с порядком применения организационных и технических мер обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду, порядком использования в образовательном процессе цифровых образовательных ресурсов;

с документами национальной системы стандартизации, действующими в области защиты информации;

знать:

содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

основные виды угроз безопасности персональных данных в информационных системах персональных данных;

содержание и порядок организации работ по выявлению угроз безопасности персональных данных;

процедуры задания и реализации требований по защите информации в информационных системах персональных данных;

меры обеспечения безопасности персональных данных;

требования по обеспечению безопасности персональных данных;

порядок применения организационных и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

порядок применения организационных и технических мер обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду;

меры обеспечения безопасности локальной сети образовательной организации;

порядок применения организационных и технических мер обеспечения информационной безопасности детей при использовании ресурсов сети Интернет.

уметь:

планировать мероприятия по обеспечению безопасности персональных данных;

разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных;

обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;

проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных;

определять состав и содержание мер по обеспечению информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду;

определять состав и содержание мер по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет.

ИМЕТЬ НАВЫК:

определения уровня защиты персональных данных;
выявления угроз безопасности персональных данных в информационных системах персональных данных;

применения организационных мер и программно-аппаратных средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных от несанкционированного доступа;

применения организационных мер и программно-аппаратных средств обеспечения информационной безопасности образовательных учреждений в контексте противодействия угрозам терроризма, экстремизма и противодействию суициду.

применения организационных мер по обеспечению информационной безопасности детей при использовании ресурсов сети Интернет.