**Аннотация дополнительной профессиональной программы (программы повышения квалификации) «Обеспечение информационной безопасности организации»**

***Актуальность.*** Отличительной особенностью современности является переход от индустриального общества к информационному, в котором главным ресурсом становится информация. Конфиденциальность, целостность, доступность информации являются одними из основных её свойств для надёжного функционирования любой организации. Соблюдением этих свойств является процесс обеспечения информационной безопасности.

Для любой организации в современных условиях одной из главных задач является обеспечение защиты информации. Важным направлением защиты информации является защита персональных данных, которые содержатся в информационных системах персональных данных и в других источниках информации. Организация, в которой правильно организована защита информационных систем и иных источников информации, создаёт надёжную и безопасную среду для своей деятельности.

Организационные меры заключаются в формальных процедурах и правилах работы с информацией, информационными сервисами и средствами защиты. Технические меры включают в себя использование программных средств контроля доступа, мониторинг утечек и краж информации, антивирусную защиту, защиту от электромагнитных излучений и т. д.

Задачи систем информационной безопасности организации многогранны: соблюдение законодательства в области персональных данных Российской Федерации, обеспечение надёжного хранения данных на различных носителях, защита информации, передаваемой по каналам связи, ограничение доступа к некоторым данным, создание резервных копий и многое другое.

Сегодня мы наблюдаем достаточно большой спектр угроз информационной безопасности организации в любой сфере деятельности. Система обеспечения информационной безопасности не может быть ограничена только оценкой защищённости информационных ресурсов и определением уровня информационной безопасности. Полноценное обеспечение информационной безопасности организации реально только при организованной системе защиты информации. Она должна включать в себя ряд определённых действий организационного и экономического характера, позволяющих качественно повысить уровень обеспечения информационной безопасности в организации.

**Цель Программы**: совершенствования компетенций в области защиты информации, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности организации, получение допуска к работе со средствами криптографической защиты информации педагогических работников образовательных организаций, должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием, руководителей учреждений, пользователей средств криптографической защиты информации и следующих специалистов: по защите информации; ответственных за организацию обработки персональных данных; ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных

**Задачи:**

1. Ознакомление слушателей с основами информационной безопасности;
2. Формирование представления о принципах и условиях обработки персональных данных, правах субъекта и обязанностей оператора;
3. Ознакомление с Федеральным государственным контролем (надзором) за обработкой персональных данных и

ответственностью за нарушения в области персональных данных в Российской Федерации.

4. Формирование навыков по защите информации ограниченного доступа с использованием средств криптографической защиты информации.

**Категория слушателей:** педагогические работники образовательных организаций, специалисты по защите информации, должностные лица, ответственные за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием, специалисты, ответственные за организацию обработки персональных данных, специалисты, ответственные за обеспечение безопасности персональных данных в информационных системах, пользователи средств криптографической защиты информации.

**Требования к квалификации и уровню подготовки слушателей:** слушатели, обучающиеся по данной Программе, должны иметь высшее или среднее профессиональное образование, без предъявления требований к стажу работы.

**Характеристика источников, использованных для разработки Программы:** нормативные, нормативно-правовые документы, методологические документы федерального и регионального уровней. Источники, использованные для разработки Программы, представлены в списке литературы.

**Описание перечня профессиональных компетенций в рамках имеющейся квалификации, изменение которых осуществляется в результате обучения по дополнительной профессиональной программе:** для формирования информационно-управленческой культуры слушателям – руководителям и педагогическим работникам образовательных организаций, руководителям и специалистам органов управления образования, осуществляющим управление в сфере образования, специалистам МОУО, претендующих на участие в процедурах и мероприятиях в сфере государственной регламентации образовательной деятельности – в условиях цифровой

образовательной среды на этапе цифровой трансформации образования необходимо совершенствовать группы компетентностей (правовая, организационная, техническая), каждая из которых формируется через все разделы и темы учебного плана и рабочей программы.

**Трудоемкость освоения Программы:** 40 часов на слушателя.

**Особенности реализации Программы в различных формах обучения и срок освоения:** формы обучения слушателей по Программе: очная, очная с использованием электронного обучения, дистанционных образовательных технологий.

Учебные план и учебно-тематические планы, приведённые в Программе, могут изменяться в зависимости от образовательных потребностей слушателей и условий реализации Программы. Любые изменения утверждаются локальными актами ГБУ ДПО РЦОКИО.

## Планируемые результаты освоения Программы

| Планируемые результаты реализации Программы | Перечень формируемых у слушателей компетенций в ходе реализации Программы |
|---|---|
| **Актуализация знаний и понимания**<br>*Знать:*<br>содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;<br>основные виды угроз безопасности персональных данных в информационных системах персональных данных;<br>содержание и порядок организации работ по выявлению угроз безопасности персональных данных;<br>процедуры задания и реализации требований по защите информации в информационных системах персональных данных;<br>меры обеспечения безопасности персональных данных;<br>требования по обеспечению безопасности персональных данных;<br>порядок применения организационных мер и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных; | **Профессиональные компетенции**<br>**Правовые:**<br>применение навыков использования определённых нормативных и правовых документов в ходе решения задач, связанных с обеспечением информационной безопасности и обработкой информации;<br>принятие правовых, организационных и технических мер по защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;<br>**Организационные:**<br>разработка предложений по совершенствованию и повышению эффективности принимаемых мер по защите персональных данных;<br>защита информации ограниченного доступа с использованием средств криптографической защиты информации.<br>**Технические:** |

| Планируемые результаты реализации Программы | Перечень формируемых у слушателей компетенций в ходе реализации Программы |
|---|---|
| нормативные правовые акты Российской Федерации по эксплуатации средств криптографической защиты информации, об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с их использованием конфиденциальной информации<br>*Уметь:*<br>планировать мероприятия по обеспечению безопасности персональных данных;<br>разрабатывать необходимые документы по обеспечению безопасности персональных данных;<br>обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;<br>проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;<br>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;<br>определять уровень защищенности персональных данных;<br>выявлять угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;<br>эксплуатировать средства криптографической защиты информации. | разработка технических требований и технических заданий на защищаемые информационные системы;<br>выявление возможных источников и каналов утечки информации;<br>разработка технических заданий на создание системы и (или) модели угроз безопасности информации, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений; |

## Содержание Программы

### Характеристика структуры Программы

Дополнительная профессиональная программа (программа повышения квалификации) «Обеспечение информационной безопасности организации» представлена следующими взаимосвязанными блоками: «Основы информационной

безопасности», «Обработка персональных данных», «Защита информации ограниченного доступа с использованием средств криптографической защиты информации».

**Первый раздел** «Основы информационной безопасности» знакомит слушателей с основными понятиями в области информации, персональных данных и информационной безопасности. В разделе раскрываются особенности и свойства информации, формы её представления, приводится классификация информации по категории доступа. В данном разделе приводится обзор нормативных, нормативных правовых актов Российской Федерации и рекомендаций в области информации, персональных данных и защиты информации.

**Второй раздел** «Обработка персональных данных» позволяет сформировать у слушателей представление о принципах и условиях обработки персональных данных, правах субъекта персональных данных и обязанностях оператора. В данном разделе даётся представление о Федеральном государственном контроле (надзоре) за обработкой персональных данных и рассматривается ответственность за нарушение законодательства Российской Федерации в области персональных данных.

**Третий раздел** «Защита информации ограниченного доступа с использованием средств криптографической защиты информации» даёт представление о нормативных правовых актах Российской Федерации по эксплуатации средств криптографической защиты информации, об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с их использованием конфиденциальной информации. В данном разделе рассматривается эксплуатация средств криптографической защиты информации. Раздел нацелен на формирование навыков по защите информации ограниченного доступа с использованием средств криптографической защиты информации, в том числе с применением электронной подписи.

**Особенности реализации Программы в различных формах работы со слушателями**

Программа предусматривает проведение лекционных, практических (в том числе лабораторные и семинарские занятия) с использованием электронного обучения и дистанционных образовательных технологий. Соотношение лекционных и практических занятий обусловлено ориентацией на формирование как теоретической, так и практической подготовки. При организации учебного процесса большинство времени отводится на проведение практических занятий с использованием интерактивных методов обучения, основанных на деятельностных и диалоговых формах познания.

Особенности реализации Программы отражены в методических рекомендациях по проведению учебных занятий. Они могут быть расширены и углублены преподавателями в зависимости от образовательной ситуации.

## Учебный план
## дополнительной профессиональной программы
## (программы повышения квалификации)
## «Обеспечение информационной безопасности организации»

**Цель:** совершенствования компетенций в области защиты информации, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности организации, получение допуска к работе со средствами криптографической защиты информации педагогических работников образовательных организаций, должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием, руководителей учреждений, пользователей средств криптографической защиты информации и следующих

специалистов: по защите информации; ответственных за организацию обработки персональных данных; ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных

**Категория слушателей**: педагогические работники образовательных организаций, специалисты по защите информации, должностные лица, ответственные за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием, специалисты, ответственные за организацию обработки персональных данных, специалисты, ответственные за обеспечение безопасности персональных данных в информационных системах, пользователи средств криптографической защиты информации.

**Трудоемкость программы**: 40 часов.

**Форма обучения**: очная, очная с использованием электронного обучения, дистанционных образовательных технологий.

**Календарный учебный график:** количество дней определяется трудоемкостью из расчета 8 часов в день, стационарное и дистанционное обучение.

| № п/п | Наименование разделов | Трудоемкость программы, ч. | Форма контроля |
|---|---|---|---|
| | | 40 | |
| 1. | Основы информационной безопасности | 6 | Входная диагностика |
| 2. | Обработка персональных данных | 26 | |
| 3. | Защита информации ограниченного доступа с использованием средств криптографической защиты информации | 6 | Итоговая диагностика |
| 4. | Итоговая аттестация | 2 | Тест |
| | **Итого:** | **40** | |