**Техническое задание**

Автономная некоммерческая организация дополнительного профессионального образования «Корпоративный Университет «ЕвроСибЭнерго» (АНО ДПО КУ ЕСЭ) приглашает принять участие в закупке на проведение обучения для руководителей и специалистов на тему **«Информационная безопасность»**, в соответствии с техническим заданием (Приложение 1).

Требуется проведение обучения для руководителей и специалистов по теме **«Информационная безопасность» (**в соответствии с техническим заданием, Приложение 1), рассматривается проведение обучения в двух вариантах\*:

1. очный формат обучения (г. Иркутск, ул. Карла Либкнехта, 28);
2. дистанционном онлайн-формате (вебинар).

\*Заказчик оставляет за собой право корректировать сроки обучения и выбирать формат обучения (очный или дистанционный онлайн-формат);

1. **Условия, предъявляемые по потенциальному поставщику услуг:**

* Лицензия на осуществление образовательной деятельности (в случае, если данный вид обучения подлежит лицензированию);
* Выдача удостоверения / свидетельства о повышении квалификации при условии успешного прохождения курса;

1. **В коммерческом предложении должно отражаться:**

* цена услуг без НДС с учетом всех возможных затрат (в двух вариантах: **очное обучение** (в г. Иркутске) и **вебинар** (дистанционное-онлайн обучение);
* условия оплаты;
* резюме преподавателя/преподавателей (опыт, квалификация, компетенции);
* график/расписание занятий/консультаций;
* программа курса должна соответствовать тем. плану обучения (раздел III);
* образец документа, выдаваемого слушателю в случае успешного освоения курса должен соответствовать установленному образцу (удостоверение/свидетельство о повышении квалификации).

1. **Тематический план обучения**

**Субъекты и объекты информационной инфраструктуры**

* Основные понятия, определения и термины.
* Сфера действия закона.

**Общие требования законодательства в сфере КИИ**

* Правовое регулирование.
* Принципы обеспечения безопасности КИИ (законность, непрерывность, комплексность, приоритет предотвращения компьютерных атак).

**Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)**

* Состав сил и средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
* Национальный координационный центр по компьютерным инцидентам.
* Реестр значимых объектов КИИ.
* Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области ОБ КИИ (Правительство РФ, ФСБ России, ФСТЭК России и Министерства связи и массовых коммуникаций).
* Перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
* Порядок представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
* Порядок обмена информацией о компьютерных инцидентах.
* Права и обязанности субъектов критической информационной инфраструктуры.
* Оценка безопасности критической информационной инфраструктуры.
* Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.
* Форма акта проверки, составляемого по итогам проведения проверки КИИ.
* Ответственность за нарушение требований.

**Категорирование объектов КИИ**

* Категории значимости объектов.
* Виды критериев и порядок отнесения объектов к категориям значимости.
* Представление информации в реестр и ведение реестра значимых объектов КИИ.
* Формы направления сведений о результатах категорирования объектов КИИ.
* Порядок и основания изменения категорий значимости

**Система безопасности значимого объекта КИИ**

* Основные задачи системы безопасности (предотвращение неправомерного доступа, а также иных неправомерных действий в отношении такой информации; недопущение воздействия на технические средства обработки информации; восстановление функционирования значимого объекта; непрерывное взаимодействие с государственной системой).
* Угрозы безопасности КИИ.
* Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.
* Требования к силам обеспечения безопасности значимых объектов критической информационной инфраструктуры.
* Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры.
* Угрозы безопасности КИИ.
* Требования к организационно-распорядительным документам по безопасности значимых объектов.
* Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

**Состав мер по обеспечению безопасности и их базовые наборы для соответствующей категории значимого объекта КИИ**

* Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов
  + Установление требований к обеспечению безопасности значимого объекта
  + Разработка организационных и технических мер по обеспечению безопасности значимого объекта
  + Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
  + Обеспечение безопасности значимого объекта в ходе его эксплуатации
  + Обеспечение безопасности значимого объекта при выводе его из эксплуатации
* Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов
* Cостав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости:
  + Идентификация и аутентификация (ИАФ)
  + Управление доступом (УПД)
  + Ограничение программной среды (ОПС)
  + Защита машинных носителей информации (ЗНИ).
  + Аудит безопасности (АУД)
  + Антивирусная защита (АВЗ)
  + Предотвращение вторжений (компьютерных атак) (СОВ)
  + Обеспечение целостности (ОЦЛ)
  + Обеспечение доступности информации (ОДТ)
  + Защита технических средств и систем (ЗТС)
  + Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
  + Реагирование на инциденты информационной безопасности (ИНЦ)
  + Управление конфигурацией (УКФ)
  + Управление обновлениями программного обеспечения (ОПО)
  + Планирование мероприятий по обеспечению безопасности (ПЛН)
  + Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
  + Информирование и обучение персонала (ИПО)

**Меры повышения уровня ИБ через совершенствование инфраструктуры.**

* Реализация общей концепции ИБ организации. Выстраивание процессов обеспечения информационной безопасности организации КИИ.
* Установление требований к обеспечению безопасности значимого объекта КИИ.
* Построение безопасной инфраструктуры. Сегментация инфраструктуры. Внедрение систем мониторинга инфраструктуры.
* Разработка и планирование организационных и технических мер по обеспечению безопасности значимого объекта.
* Установление требований к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов.
* Внедрение необходимых контролей и метрик эффективности работы процессов обеспечения информационной безопасности.
* Анализ угроз безопасности информации и уязвимостей, которые могут привести к компьютерным инцидентам на объекте КИИ.
* Оценка возможных последствий компьютерных инцидентов на объектах.
* Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.

**Состав требований и мер по обеспечению безопасности и их базовые наборы для соответствующей категории значимого объекта КИИ**

* Определение вида и типа программных, программно–аппаратных средств защиты информации, обеспечивающих реализацию технических мер по защите значимого объекта КИИ.
* Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие.
* Обеспечение безопасности значимого объекта в ходе его эксплуатации.
* Обеспечение безопасности значимого объекта при выводе его из эксплуатации.
* Реализация требований к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов.
* Характеристика организационных и технических мер, направленных на блокирование (нейтрализацию) угроз безопасности информации:
  + Идентификация и аутентификация (ИАФ)
  + Управление доступом (УПД)
  + Ограничение программной среды (ОПС)
  + Защита машинных носителей информации (ЗНИ)
  + Аудит безопасности (АУД)
  + Антивирусная защита (АВЗ)
  + Предотвращение вторжений (компьютерных атак) (СОВ)
  + Обеспечение целостности (ОЦЛ)
  + Сопоставление и взаимная увязка требований к защите в случаях, когда в КИИ присутствуют сразу к нескольким категорий ГИС, АСУ ТП или ПДн.
  + Обеспечение доступности информации (ОДТ)
  + Защита технических средств и систем (ЗТС)
  + Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
  + Реагирование на инциденты информационной безопасности (ИНЦ)
  + Управление конфигурацией (УКФ)
  + Управление обновлениями программного обеспечения (ОПО)
  + Планирование мероприятий по обеспечению безопасности (ПЛН)
  + Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
  + Информирование и обучение персонала (ИПО)
* Сопоставление и взаимная увязка требований к защите в случаях, когда в КИИ присутствуют сразу к нескольким категорий ГИС, АСУ ТП или ПДн.

**Обзор рынка технических средств защиты информации (СЗИ), покрывающих требования законодательства по защите КИИ**

* Рекомендованный состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости.
* Основные методы и способы защиты от НСД.
* Методики аттестационных испытаний системы защиты от несанкционированного доступа.
* Методики прохождения оценки соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании».
* Оценка уровней защищенности для отдельных технических средств и каналов утечки информации.
* Сравнительный анализ решений от разработчиков СЗИ, предлагаемых на российском рынке. Функционал. Практические кейсы.

**II. Целевая аудитория:**

1. Инженерно-технические работники (руководители и специалисты).

2. Количество участников обучения – не более 40 чел.

**III. Возможные варианты форматов проведения обучения:**

1. Очное групповое обучение в г. Иркутске.

2. Вебинар (Дистанционное групповое онлайн-обучение).

IV. **Дополнительные требования для проведения обучения**

**Вариант 1, формат вебинара** (дистанционный онлайн-формат):

1. Электронная платформа (указать наименование) с возможностью:

* демонстрации контента (презентации, видео- / аудиоматериалов);
* двусторонней аудио- / видеосвязи преподавателя и слушателей;
* писать вопросы преподавателю в чат;
* отображения статистики посещаемости слушателей;

1. Скорость интернет-соединения от 5 Мбит/с.;
2. Обеспечение технической поддержки со стороны администратора / IT-специалиста (указать контакты для оперативного взаимодействия в случае неисправности);

*Важно: за 3 рабочих дня до наступления срока проведения вебинара администратор / IT-специалист проводит тестовое подключение рабочих мест слушателей к электронной площадке (время определяется по согласованию с Заказчиком).*

1. Ведение записи вебинара / видеотрансляции (требования к записи: формат видеофайла – mp4; видеокодек - H.264; аудиокодек – AAC; max объем файла – не более 1 Гб).
2. Время проведения занятий: в период с 08.30 до 12.00 МСК (с понедельник по четверг), с 08.30 до 11.00 МСК (в пятницу);
3. Обязательный разбор материалов во время проведения вебинара, ответы преподавателя на вопросы слушателей, возникающие в процессе обучения;
4. консультационные часы преподавателя в течение двух недель после завершения обучения (график определяется по согласованию с Заказчиком).

**Вариант 2**, очный формат:

1. В соответствии с действующим законодательством РФ для проведения аудиторных занятий предусмотреть:

* академический час устанавливается продолжительностью 45 минут;
* объем обязательных аудиторных занятий не должен превышать 36 академических часов в неделю;
* время проведения занятий с 09:00 до 16:00 с перерывом на обед (с 12:00 до 13:00) – в соответствии с Правилами внутреннего распорядка АНО ДПО КУ ЕСЭ;

1. Соблюдение учебной дисциплины;
2. Предоставление материалов курса (к примеру: презентация, раздаточный материал, брошюры, памятки, методички, схемы и т.д.)
3. Обязательный разбор материалов во время проведения аудиторных занятий,
4. Ответы преподавателя на вопросы слушателей, возникающие в процессе обучения;
5. Консультационные часы преподавателя в течение двух недель после завершения обучения (график определяется по согласованию с Заказчиком).

\* Аудиторию для проведения очных занятий предоставляет Заказчик.

**V. Сроки оказания услуг** - обучение должно быть завершено не позднее 29 июня 2023 г.

|  |  |  |
| --- | --- | --- |
| С уважением,  Заместитель директора по организационному развитию |  | А.Я. Ранцан |