

Конфиденциально

Коммерческое предложение

на оказание услуг по категорированию
объектов КИИ

подготовлено для:
ООО "ЭЛЕКТРОСЕТИ"

Представитель Заказчика:
Дмитрий Борисов
+7 382 354-09-36
borisov@els-seversk.ru

Представитель Исполнителя:
Ольга Соборникова
Тел: +7 (495) 108-71-52
o.sobornikova@data-sec.ru

Дата составления: 20.02.2025

Срок действия коммерческого предложения – 2 месяца

Коротко о Центре безопасности данных

Центр безопасности данных является профессиональным интегратором решений по внедрению систем информационной безопасности, защиты персональных данных и безопасности критической информационной инфраструктуры «под ключ». Наш коллектив состоит из молодых IT-специалистов с высшим техническим образованием со специализациями в области информационной безопасности, защиты информационных систем, сетей данных и систем автоматизации.

Центральный офис компании находится в г. Тольятти Самарской области.
ООО ЦБД «Айдеко», ОГРН 1116324006710, ИНН 6324020784, КПП 632401001

При работе с клиентом для нас важно:

- ✓ быть удобным для клиента;
- ✓ быть открытым и честным с клиентом;
- ✓ вникать в потребности клиента;
- ✓ подбирать решения оптимальные по цене и качеству;
- ✓ сопровождать клиента на всем процессе внедрения и использования систем информационной безопасности;
- ✓ внедрять решения, которые будут удовлетворять требованиям информационной безопасности.

С нами легко работать и нам можно доверять!



23 августа 2012 г. мы получили **бессрочную** лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации

Реквизиты лицензии:

Серия КИ 0228 № 011480

Регистрационный № 1828 от 23 августа 2012 г.

Лицензия предоставлена на основании приказа ФСТЭК России от 23 августа 2012 г. № 174-л

Предлагаемая схема работы

- ✓ Заключаем договор возмездного оказания услуг по подготовке сведений о результатах присвоения объекту КИИ одной из категории значимости.
- ✓ Вы предоставляете нам сведения, необходимые для оказания услуг, путем заполнения несложных опросных листов и интервьюирования.
- ✓ Мы **осуществляем подготовку** организационно-распорядительных документов, регламентирующих работу комиссии по категорированию, работу ответственных за обеспечение безопасности объектов КИИ, актов категорирования.
- ✓ Подготавливаем сведения о результатах присвоения объекту КИИ одной из категории значимости / отсутствии необходимости присвоения ему одной из таких категорий, в соответствии со 127 Постановлением Правительства РФ и 236 приказом ФСТЭК. Разрабатываем уведомление о категорировании объектов КИИ для направления во ФСТЭК, в соответствии со 127 Постановлением Правительства РФ.
- ✓ Направляем в ваш адрес разработанные документы в электронном виде. Вам останется **только распечатать, утвердить и внедрить** их.
- ✓ Бухгалтерские и иные отчетные документы направляются в ваш адрес почтой либо с использованием электронного документооборота (ЭДО).

Этапы работ

С целью выполнения требований действующего законодательства в области безопасности критической информационной инфраструктуры (КИИ) Российской Федерации, в части обязательных работ по категорированию объектов КИИ предполагается проведение следующих этапов работ:

Этап 1:

- *Обследование инфраструктуры Заказчика. Разработка документов о назначении комиссии по категорированию, о назначении уполномоченного в области обеспечения безопасности объектов КИИ, а также положений, регламентирующих их работу.* Обследование может носить очный либо дистанционный характер. Дистанционное обследование проводится путем анкетирования (заполнения опросных листов и анализ предоставленных сведений Заказчиком) и интервьюирования Заказчика. Оно характерно для малых и средних организаций. Для крупных организаций со сложной информационной архитектурой применим только очный характер обследования. В этом случае работы по обследованию инфраструктуры Заказчика выделяют отдельным этапом и оформляют отдельным договором,

так как объем работ по проведению категорирования объектов КИИ определить невозможно.

- *Подготовка сведений о результатах присвоения объекту КИИ одной из категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий* Разработка актов о категорировании объектов КИИ, уведомления о результатах категорирования объектов КИИ Заказчика для направления во ФСТЭК в соответствии с Постановлением Правительства РФ N 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" и Приказом ФСТЭК России № 236 "Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий".

Этап 2:

- *Проектирование системы обеспечения информационной безопасности (СОИБ)* в соответствии с Приказом ФСТЭК России от 21.12.2017 N 235 (ред. от 20.04.2023) "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования" и Приказом ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ».

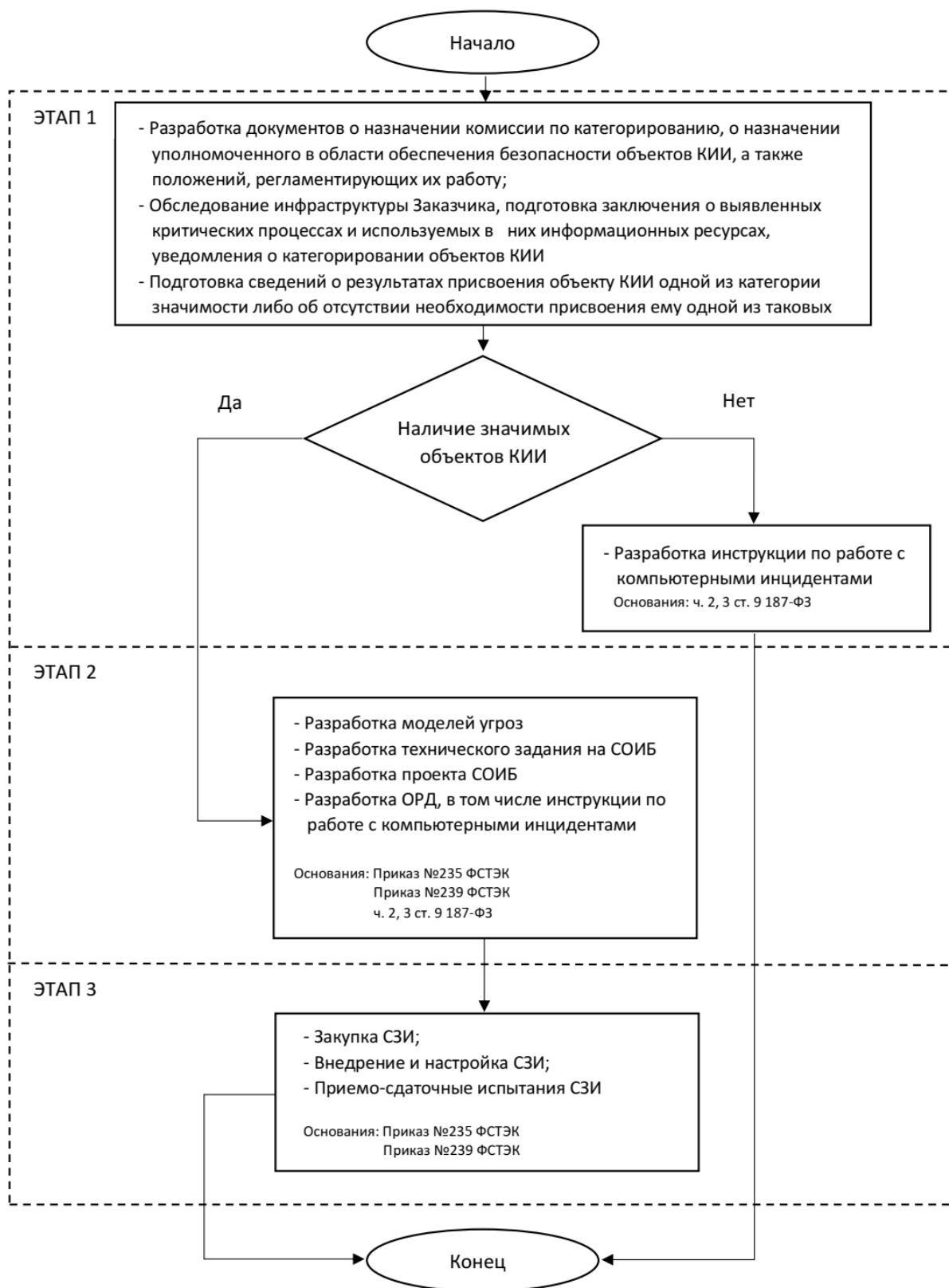
Этап 3:

- *Реализация проекта системы обеспечения информационной безопасности (СОИБ).* Внедрение средств защиты информации (программных и аппаратных), подключение к ГосСОПКА.

Каждый этап работ проводится в рамках отдельного договора, ввиду отсутствия возможности оценки трудоемкости всего объема работы.

Графическое описание этапов реализации требований 187-ФЗ "О безопасности КИИ РФ" представлено ниже в виде блок-схемы.

Блок-схема реализации требований 187-ФЗ "О безопасности КИИ РФ"



ЭТАП 1

1.1. Обследование инфраструктуры Заказчика; Подготовка заключения о выявленных критических процессах и используемых в них информационных ресурсах, уведомления о категорировании объектов КИИ

Под данными работами предполагается:

- ✓ Разработка и согласование Приказа об учреждении комиссии по категорированию, Положения о работе комиссии по категорированию объектов КИИ;
- ✓ Разработка и согласование Приказа о назначении уполномоченного в области обеспечения безопасности объектов КИИ, Положения о работе уполномоченного в области обеспечения безопасности объектов КИИ;
- ✓ Обследование и анализ существующих бизнес-процессов организации (управленческих, технологических, производственных, финансово-экономических и иных) с целью выявления критических информационных процессов и объектов;
- ✓ Разработка Заключения о выявленных критических процессах и используемых в них информационных ресурсах.

Результатом работы будут являться:

- ✓ Приказ «О создании комиссии по категорированию объектов КИИ»;
- ✓ Положение о комиссии по категорированию объектов КИИ;
- ✓ Приказ «О лице, уполномоченном в области обеспечения безопасности объектов КИИ»;
- ✓ Положение о лице, уполномоченном в области обеспечения безопасности объектов КИИ;
- ✓ Заключение о выявлении критических процессов и используемых в них информационных ресурсах.

1.2. Подготовка сведений о результатах присвоения объекту КИИ одной из категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Работы выполняются с целью выполнения п. 17 Постановления Правительства РФ №127 от 08.02.2018г., который предписывает организациям-субъектам КИИ направить во ФСТЭК сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об

отсутствии необходимости присвоения ему одной из таких категорий. Сведения оформляются в форме, регламентируемой 236 Приказом ФСТЭК от 22.12.2017г.

Указанные сведения включают:

- ✓ сведения об объекте критической информационной инфраструктуры;
- ✓ сведения о субъекте критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит объект критической информационной инфраструктуры;
- ✓ сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи;
- ✓ сведения о лице, эксплуатирующем объект критической информационной инфраструктуры;
- ✓ сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах соответствия требованиям по безопасности информации (при наличии);
- ✓ сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта критической информационной инфраструктуры либо об отсутствии таких угроз;
- ✓ возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры либо сведения об отсутствии таких последствий;
- ✓ категорию значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;
- ✓ организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры, либо сведения об отсутствии необходимости применения указанных мер.

Под данными работами предполагается:

- ✓ Определение всех элементов критических информационных процессов, архитектуры и программно-аппаратного состава;
- ✓ Оценка возможного ущерба, причиненного в результате возникновения компьютерного инцидента на объекте КИИ – разработка экспертного заключения;

- ✓ Присвоение категории значимости объекта для каждого показателя значимости объектов КИИ – разработка Актов о категорировании объектов КИИ согласно Постановления Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- ✓ Заполнение формы Уведомления о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости для направления и согласования с ФСТЭК.
- ✓ Организация работы с инцидентами информационной безопасности согласно ч. 2, 3 ст. 9 187-ФЗ "О безопасности КИИ РФ"

Результатом работы будут являться:

- ✓ Акты категорирования объектов критической информационной инфраструктуры;
- ✓ Уведомление ФСТЭК России о результатах категорирования (заполненная форма направления сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости);
- ✓ Приказ «Об утверждении инструкции по работе с инцидентами информационной безопасности»;
- ✓ Инструкция по работе с инцидентами информационной безопасности;
- ✓ Журнал регистрации инцидентов информационной безопасности.

ЭТАП 2

2.1. Моделирование угроз безопасности значимых объектов КИИ

Работы выполняются с целью выполнения требований Приказа ФСТЭК России от 21.12.2017 N 235 (ред. от 20.04.2023) "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования" и Приказа ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ».

Под данными работами предполагается:

- ✓ Анализ угроз информационной безопасности значимых объектов КИИ;
- ✓ Формирование модели угроз ИБ и модели нарушителя ИБ для каждого значимого объекта КИИ.

2.2. Разработка технического задания и технического проекта на систему обеспечения информационной безопасности

Техническое задание на создание системы обеспечения информационной безопасности основано на проведенном категорировании объектов КИИ, моделировании угроз информационной безопасности и используемых в организации информационных ресурсах.

Технический проект системы обеспечения информационной безопасности: включает в себя:

- ✓ Пояснительную записку к техническому проекту;
- ✓ Структурную схему;
- ✓ Ведомость покупных изделий;
- ✓ Описание настроек средств защиты информации;
- ✓ Программа и методика испытаний.

2.3. Разработка организационно-распорядительных документов

В рамках данного процесса разрабатываются следующие проекты документов:

- ✓ Политика обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- ✓ Инструкция должностного лица, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры или Положение структурного подразделения ИБ (по необходимости);

- ✓ Положение о структурном подразделении, обеспечивающем информационную безопасность;
- ✓ Инструкция сотрудника структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры (при необходимости);
- ✓ Положение об идентификации и аутентификации на значимых объектах критической информационной инфраструктуры;
- ✓ Положение об управлении доступом к значимым объектам критической информационной инфраструктуры;
- ✓ Положение о правилах и процедурах ограничения программной среды в значимых объектах критической информационной инфраструктуры;
- ✓ Положение о защите машинных носителей информации в значимых объектах критической информационной инфраструктуры;
- ✓ Положение об аудите безопасности значимых объектов критической информационной инфраструктуры;
- ✓ Положение об антивирусной защите значимого объекта критической информационной инфраструктуры;
- ✓ Положение о предотвращении вторжений (компьютерных атак) на значимые объекты критической информационной инфраструктуры;
- ✓ Положение об обеспечении целостности значимых объектов критической информационной инфраструктуры;
- ✓ Положение об обеспечении доступности значимых объектов критической информационной инфраструктуры;
- ✓ Положение по защите технических средств и систем значимых объектов критической информационной инфраструктуры;
- ✓ Положение о правилах и процедурах реагирования на компьютерные инциденты, в том числе в значимых объектах критической информационной инфраструктуры;
- ✓ Положение об управлении конфигурацией значимых объектов критической информационной инфраструктуры;
- ✓ Положение о защите информационных (автоматизированных) систем и ее компонентов значимых объектов критической информационной инфраструктуры;
- ✓ Положение о правилах и процедурах планирования мероприятий по обеспечению защиты информации в значимых объектах критической информационной инфраструктуры;

- ✓ Положение об управлении обновлениями программного обеспечения объекта критической информационной инфраструктуры и средств защиты информации;
- ✓ Положение об обеспечении действий в нештатных ситуациях на значимых объектах критической информационной инфраструктуры;
- ✓ Положение о правилах и процедурах информирования и обучения персонала, эксплуатирующего и обеспечивающего функционирование значимых объектов критической информационной инфраструктуры;
- ✓ Регламент информирования ФСБ России (НКЦКИ) о компьютерных инцидентах;
- ✓ План реагирования на компьютерные инциденты в значимых объектах критической информационной инфраструктуры;
- ✓ График тренировок по отработке мероприятий плана реагирования на компьютерные инциденты;
- ✓ Регламент по выявлению, анализу и устранению критичных уязвимостей в принадлежащих организации объектах критической информационной инфраструктуры;
- ✓ Регламент по анализу и установке обновлений безопасности программных, программно-аппаратных средств объектов критической информационной инфраструктуры;
- ✓ Регламент резервного копирования и восстановления информации;
- ✓ Регламент повышения уровня безопасности информационных ресурсов;
- ✓ Порядок вывода из эксплуатации значимого объекта критической информационной инфраструктуры;
- ✓ Порядок взаимодействия подразделений при решении задач обеспечения безопасности ЗОКИИ;
- ✓ Инструкция персонала, эксплуатирующего и обеспечивающего функционирование значимых объектов критической информационной инфраструктуры;
- ✓ Инструкция по взаимодействию структурных подразделений со сторонними организациями по вопросам эксплуатации ЗОКИИ.

ЭТАП 3

3.1. Внедрение средств защиты информации (программных и аппаратных)

Под данными работами предполагается:

- ✓ Закупка средств защиты информации;
- ✓ Внедрение и настройка средств защиты информации;
- ✓ Приемо-сдаточные испытания средств защиты информации.

3.2. Подключение к ГосСОПКА

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, создаваемая в целях предотвращения и устранения последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации.

Она представляет собой иерархически взаимодействующие государственные и коммерческие центры, которые непрерывно делятся информацией о зафиксированных инцидентах и способах противодействия им.

В текущих версиях опубликованных нормативно-правовых актов нет однозначного требования об обязательности подключения к ГосСОПКА и использования для взаимодействия с ней каких-либо технических средств. Однако, для эффективной реализации требований по непрерывности взаимодействия с НКЦКИ для крупных объектов КИИ, а особенно для реализации мер из Приказа ФСТЭК №239 для значимых объектов 1 и 2 категории, на практике использование технических средств оправдано.

Под данными работами предполагается:

- ✓ Определение необходимых организационных и технических мер для подключения к ГосСОПКА;
- ✓ Определение подразделений и должностных лиц, ответственных за взаимодействие с НКЦКИ;
- ✓ Проектирование и внедрение необходимых средств ГосСОПКА;
- ✓ Разработка ОРД и регламентов;
- ✓ Подключение к технической инфраструктуре НКЦКИ.

Оценка стоимости работ по Этапу 1

Наименование этапов работ	Цена, руб.	Кол-во, ед.	Сумма, руб.
1.1 Обследование инфраструктуры Заказчика; Подготовка заключения о выявленных критических процессах и используемых в них информационных ресурсах, уведомления о категорировании объектов КИИ	105 000	1	105 000
1.2 Подготовка сведений о результатах присвоения объекту КИИ одной из категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	116 000	1	116 000

ИТОГО: 221 000.00 руб

НДС не облагается в соответствии с применением Исполнителем упрощенной системы налогообложения в соответствии с п. 2 ст. 346.11 Налогового Кодекса РФ

Сроки исполнения: 25-40 рабочих дней

Коммерческое предложение не является офертой

Данное коммерческое предложение строго конфиденциально (включая все приложения). Информация, изложенная в данном коммерческом предложении, предназначена только для получателя(ей). Если Вы не являетесь получателем, Вы не вправе каким бы то ни было образом читать, копировать, использовать, хранить или пересылать данное коммерческое предложение. Просьба немедленно его удалить.

Если Вы получили это коммерческое предложение по ошибке, пожалуйста, свяжитесь с нами по e-mail info@data-sec.ru (Центр безопасности данных «Айдеко»).