

INFOSECURITY

softline[®]
Мы всё сможем

ТЕХНИКО- КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

на работы по приведению объектов критической информационной инфраструктуры в соответствие с требованиями Федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» для ООО «Электросети»

Softline

Дербеневская наб., д.7, стр.8, г. Москва, 115114

+7 495 232-00-23, info@softline.ru, www.softline.ru

Infosecurity (a Softline company)

Преображенская пл., д. 8, г. Москва, 107061

+7 499 677-10-00, iss@in4security.com, www.in4security.com

Дата предложения:

21.02.2025

Срок действия предложения:

Место для ввода даты.

ОГЛАВЛЕНИЕ

РЕЗЮМЕ	3
ЦЕЛЬ ПРОЕКТА	3
РЕШЕНИЕ	3
ГРАНИЦЫ ПРОВЕДЕНИЯ РАБОТ	3
ЭТАПЫ	4
Этап 1. Обследование и сбор сведений об объектах КИИ.....	4
Этап 2. Категорирование объектов КИИ.....	4
ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ПОДГОТОВЛЕННЫХ ДОКУМЕНТОВ	5
ФИНАНСОВОЕ ПРЕДЛОЖЕНИЕ	5
Услуги.....	5
КОНТАКТЫ	5
О КОМПАНИЯХ.....	6
КОМАНДА ПРОЕКТА	6
ОТКРЫТЫЕ РЕФЕРЕНСЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	7

РЕЗЮМЕ

Настоящий документ представляет собой технико-коммерческое предложение по теме: «Приведение объектов критической информационной инфраструктуры в соответствие с требованиями Федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры российской федерации» для ООО «Электросети» (далее — Заказчик).

Содержание настоящего документа основано на опыте выполнения аналогичных (по предметной области, масштабу предприятия и используемых средств автоматизации) проектов.

Общая стоимость работ составит **453 726 (Четыреста пятьдесят три тысячи семьсот двадцать шесть) рублей 00 копеек**, с учетом НДС 20%, при общей длительности в **23 рабочих дней**.

ЦЕЛЬ ПРОЕКТА

1. Приведение в соответствие обеспечения безопасности объектов критической инфраструктуры требованиям законодательства РФ.
2. Минимизация рисков, связанных с проверками регуляторов.
3. Повышение внутренней дисциплины сотрудников, вовлеченных в процессы функционирования объектов критической инфраструктуры

РЕШЕНИЕ

Для достижения поставленной цели предлагаем провести следующие работы:

1. Обследование и сбор сведений об объектах КИИ
2. Категорирование объектов КИИ

ГРАНИЦЫ ПРОВЕДЕНИЯ РАБОТ

При проведении работ действуют следующие требования и ограничения:

- Заказчик обязуется своевременно уведомлять исполнителя об изменениях бизнес-процессов, IT-инфраструктуры и мер защиты информации, входящих в область проведения работ.
- Интервьюирование работников проводится очно на территории центрального офиса Заказчика по адресу: удаленно с использованием средств связи (телефон, Skype и т.п.).
- Область проведения работ включает: ООО «Электросети»
- Согласование разработанных документов составляет не более 5 рабочих дней с момента их предоставления Заказчику и не более 3 итераций.
- Количество информационных систем не более 2
- Количество автоматизированных систем управления технологическим процессом (АСУ ТП) не более 2

ЭТАПЫ

Этап 1. Обследование и сбор сведений об объектах КИИ

На данном этапе проводится детальное обследование бизнес-процессов, IT-инфраструктуры и действующих мер защиты информации.

Сбор сведений проводится в форме интервьюирования и (или) в форме анкетирования с использованием опросных листов. При сборе информации также проводится анализ организационно-распорядительной документации, регламентирующей ИБ и IT-процессы Заказчика.

Данный этап включает в себя следующие работы:

- сбор информации об адресах размещения объектов КИИ;
- сбор информации о должностных лицах и структурных подразделениях, ответственных за обеспечение безопасности объектов КИИ, о лицах и структурных подразделениях, эксплуатирующих объекты КИИ (при наличии);
- сбор информации об архитектуре объектов КИИ, автоматизированных рабочих местах, серверах, активном сетевом и телекоммуникационном оборудовании, обеспечивающем выполнение функций объекта КИИ по его назначению;
- определение порядка взаимодействия объектов КИИ с другими информационными системами, включая взаимодействие с другими объектами КИИ, цели и способе взаимодействия объектов КИИ с сетями электросвязи;
- определение реализованных организационных и технических мер, применяемых для обеспечения безопасности объектов КИИ, перечня применяемых средств защиты информации и наличия сертификатов ФСТЭК России и (или) ФСБ России.

Результаты этапа

Результатом этапа являются:

- перечень объектов КИИ;
- приказ о создании комиссии по категорированию объектов КИИ.

Этап 2. Категорирование объектов КИИ

На данном этапе выполняются следующие работы:

- определение категорий нарушителей, их основных возможностей и их действий в отношении объектов КИИ;
- анализ возможных угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ или обоснование их неактуальности;
- определение возможных последствий в случае возникновения компьютерных инцидентов;
- оценку масштаба последствий в случае возникновения компьютерных инцидентов;
- присвоение категории значимости объектам КИИ либо принятие решения об отсутствии необходимости присвоения категории значимости в соответствии с показателями

значимости, указанными в Перечне показателей значимости и обоснование полученных значений или их отсутствия.

Результаты этапа

Результатом этапа являются:

- акт категорирования объекта (объектов) КИИ;
- сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (для отправки во ФСТЭК России).

ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ПОДГОТОВЛЕННЫХ ДОКУМЕНТОВ

По предварительному согласованию состав и наименования разрабатываемых документов могут быть изменены в ходе выполнения работ.

Согласование документов в процессе их подготовки будет осуществляться дистанционно с использованием возможностей электронной почты в режиме одновременной рассылки электронных версий документов всем заинтересованным сторонам.

По завершении всех работ документация будет предоставлена в печатном (один экземпляр) и в электронном виде (один экземпляр). Электронный вид документов будет соответствовать формату редактора Microsoft Word.

ФИНАНСОВОЕ ПРЕДЛОЖЕНИЕ

Услуги

№	Наименование услуг	Длительность, раб. дней	Стоимость с НДС, руб.
1	Определение критических процессов и перечня объектов КИИ	13	274 985
2	Категорирование объектов КИИ	10	178 741
	Итого:	23	453 726

** Длительность представлена в рабочих днях. Сроки выполнения работ могут сдвигаться на время, необходимое Вам для предоставления информации и обратной связи.*

*** Оплата осуществляется по схеме: 50% — предоплата от стоимости этапа, 50% по завершению работ в течении 10-ти (десяти) рабочих дней с даты завершения работ и подписания акта сдачи-приёмки.*

КОНТАКТЫ

Лавроненкова Анастасия Геннадьевна,
Менеджер
+7 903 553-18-04
lavronenkova@in4security.com

О КОМПАНИЯХ

Softline — лидирующий международный поставщик ИТ-решений и сервисов, работающий на рынках России, СНГ, Латинской Америки, Индии и Юго-Восточной Азии. Мы предлагаем комплексные технологические решения, лицензирование программного обеспечения, аппаратное обеспечение и ИТ-услуги. Собственная облачная платформа Softline обеспечивает клиентов доступом к публичным, частным и гибридным облачным решениям.

Клиенты Softline — это более 60 000 частных и государственных организаций всех масштабов — от крупных холдингов до СМБ. Более 1000 аккаунт-менеджеров и маркетологов, 800 инженеров и разработчиков обслуживают наших заказчиков и помогают им выбрать оптимальные ИТ-решения. Softline — клиентоориентированная компания: мы всегда находимся на стороне клиента и предлагаем решения, наилучшим образом решающие его задачи, вне зависимости от бренда. Подробнее — на softline.ru.

Infosecurity — специализированный сервис-провайдер, оказывающий услуги в сфере информационной безопасности, ИТ и консалтинга, лицензиат ФСБ России и ФСТЭК России, входит в группу компаний Softline.

Ключевые сервисы Infosecurity — реагирование на инциденты информационной безопасности, предотвращение утечек данных (DLP), защита от угроз нулевого дня, поддержка ИТ-инфраструктуры. Компания успешно внедряет и сопровождает системы защиты информации в различных отраслях — финансы, промышленность, государственный сектор, медицина и др.

Infosecurity является членом международной федерации FIRST, а собственный центр мониторинга и реагирования на инциденты информационной безопасности (Infosecurity CERT) лицензирован университетом Карнеги-Меллон. Компания развивает свои решения — сервис выявления угроз для бизнеса (ETHIC) и Центр мониторинга и реагирования на инциденты (SOC). В отдельное направление выделено внедрение и аналитическая поддержка DLP-систем, сервис по управлению навыками ИБ (TRAINING CENTER). Подробнее — на in4security.com.

КОМАНДА ПРОЕКТА

Команда состоит из 30 аналитиков-консультантов с высшим образованием в области ИБ. Команда завершила более 100 проектов по защите объектов критической инфраструктуры и АСУ ТП за 5 лет.

ОТКРЫТЫЕ РЕФЕРЕНСЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ



Модернизация и
обеспечение
безопасности
объектов КИИ
каскада
гидроэлектростанций



Проектирование
СОИБ КИИ и
внедрение средств
защиты



Комплекс проектов
по обеспечению
безопасности
объектов
критической
инфраструктуры



Проектирование СОИБ
КИИ



Полный цикл работ



Выявление и
Категорирование
объектов
критической
инфраструктуры



Проектирование
систем защиты
персональных данных
и критической
информационной
инфраструктуры



Проектирование
системы защиты
критической
информационной
инфраструктуры