Ростелеком
Солар

Комплекс услуг по приведению организации в соответствие с требованиями 187-ФЗ «О безопасности КИИ РФ»

- Обследование инфраструктуры (аудит)
- Методологическая экспертная поддержка категорирования объектов КИИ
- Создание системы безопасности значимых объектов КИИ
- Оценка соответствия (при необходимости аттестация) значимых объектов КИИ
- Организация взаимодействия объектов КИИ с ГосСОПКА

Организации, столкнувшиеся с необходимостью исполнения ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации», часто испытывают проблемы при категорировании, проектировании и построении систем обеспечения безопасности объектов критической информационной инфраструктуры (КИИ).

Компания «Ростелеком-Солар» предлагает комплекс услуг и сервисов по приведению организации в соответствие с требованиями законодательства по обеспечению безопасности объектов КИИ.

1. Обследование инфраструктуры (аудит)
2. Методологическая экспертная поддержка категорирования объектов КИИ
3. Создание системы безопасности значимых объектов КИИ
4. Оценка соответствия (при необходимости аттестация) значимых объектов КИИ
5. Организация взаимодействия объектов КИИ с ГосСОПКА

Все услуги и сервисы соответствуют требованиям российского законодательства.

Федеральные законы

1. № 187-ФЗ от 26.07.2017 «О безопасности КИИ РФ».
2. № 193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием 187-ФЗ «О безопасности КИИ РФ».
3. Федеральные законы, регламентирующие вопросы безопасности в сферах и областях действия субъектов КИИ.

Указы Президента РФ

1. № 803 от 03.02.2012 «Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ».
2. № 646 от 05.12.2016 «Об утверждении Доктрины ИБ РФ».
3. № 31с от 15.01.2013 «О создании ГосСОПКА».
4. № 620 от 22.12.2017 «О совершенствовании ГосСОПКА».
5. № К 1274 от 12.12.2014 «О Концепции ГосСОПКА».

Постановления Правительства РФ

1. № 127 от 08.02.2018 (ред. от 13.04.2019 № 452) «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений».
2. № 162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ».
3. № 808 от 11.07.2018 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК».

Приказы ФСТЭК России

1. № 227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ».
2. № 229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ».
3. № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования».
4. № 236 от 22.12.2017 (ред. от 21.03.2019) «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
5. № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ».
6. № 72 от 26.04.2018 «О внесении изменений в Регламент ФСТЭК России».

Методические документы

1. Рекомендации № 149/2/7-200 от 24.12.2016 «Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА».
2. «Временный порядок включения корпоративных центров в ГосСОПКА».
3. Информационное сообщение ФСТЭК России № 240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ».

1 Обследование (аудит) инфраструктуры

Работы

- Очное или заочное обследование (аудит).
- Оценка защищенности инфраструктуры заказчика.
- Проверка корректности собранных заказчиком исходных данных.

Результат

- Подготовлен отчет об обследовании.
- Сформирован перечень объектов КИИ.

2 Методологическая поддержка категорирования объектов КИИ

Работы

- Анализ угроз безопасности и/или разработка модели угроз и нарушителя.
- Оценка потенциального ущерба в соответствии с критериями значимости возможных последствий компьютерных инцидентов на объектах КИИ.
- Присвоение каждому объекту КИИ категории значимости.
- Подготовка результатов категорирования к отправке во ФСТЭК России.

Результат

- Определены и задокументированы угрозы и нарушители безопасности информации.
- Подготовлены внутренние акты по результатам категорирования.
- Подготовлены формы предоставления во ФСТЭК России сведений о результатах категорирования.

3 Создание системы безопасности значимых объектов КИИ*

Работы

- Разработка технического задания на создание системы безопасности.
- Проектирование системы безопасности.
- Разработка рабочей (эксплуатационной) документации.
- Разработка комплекта организационно-распорядительной документации.
- Поставка средств защиты.
- Внедрение организационных и технических мер.

Результат

- Система безопасности спроектирована.
- Разработан комплект организационно-распорядительной документации.
- Система безопасности введена в эксплуатацию.

*Создание и внедрение системы безопасности проводится в том числе с учетом типа значимого объекта КИИ (ГИС, ИСПДн, АСУ ТП и т. д.)

4 Оценка соответствия (при необходимости аттестация) значимых объектов КИИ

Работы

- Определение формы оценки соответствия.
- Разработка программы и методики испытаний.
- Проведение испытаний системы безопасности.
- Оформление результатов испытаний.
- Оформление заключения по оценке соответствия.

Результат

- Разработана программа и методика испытаний.
- Проведены испытания и оценка соответствия.
- Выданы документы, подтверждающие соответствие объектов КИИ.

5 Организация взаимодействия объектов КИИ с ГосСОПКА

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» все объекты КИИ, включая незначимые, должны быть подключены к ГосСОПКА, созданной в рамках Указа Президента РФ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

Для подключения объектов КИИ к ГосСОПКА могут использоваться ведомственные и/или корпоративные центры, призванные осуществлять мониторинг, анализ и расследование инцидентов, анализ защищенности и целый ряд других функций.

В рамках работ по организации взаимодействия объектов КИИ с ГосСОПКА предлагаются следующие услуги:

- предоставление ресурсов Solar JSOC для автоматизации выявления и предотвращения компьютерных атак;
- построение программно-аппаратной платформы и методической базы для функционирования ведомственного или корпоративного центра ГосСОПКА;
- организация процессов выявления и предотвращения компьютерных атак, включая взаимодействие с головным центром ГосСОПКА, организованным на базе ФСБ России;
- предоставление под ключ услуг по обеспечению защиты объектов КИИ от компьютерных атак и взаимодействию с ФСБ России;
- подключение всех объектов КИИ к ГосСОПКА.

«Ростелеком-Солар» имеет все необходимые разрешения и лицензии для оказания услуг

- Лицензию ФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну
- Лицензию ФСБ России на разработку, производство и распространение шифровальных средств, информационных систем и т. д.
- Лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации.
- Лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

В результате оказания полного комплекса услуг организация сможет провести все необходимые мероприятия в рамках действующего законодательства по защите КИИ.

Ростелеком Солар

+7 (499) 755-07-70

info@rt-solar.ru rt.ru rt-solar.ru

9.08.BL.187.01