Техническое задание

1. Общие положения

Настоящее техническое задание подготовлено для целей оказания услуг по сопровождению процессов обеспечения информационной безопасности критической информационной инфраструктуры (КИИ).

* 1. Условия оказания услуг

Услуги оказываются для юридического лица Заказчика.

Услуги оказываются дистанционно, в режиме технической поддержки через портал технической поддержки, по телефону, электронной почте и (или) иным согласованным каналам коммуникации.

Порядок оказания Услуг предусматривает выполнение Исполнителем сформированных Заказчиком заявок.

Период оказания Услуг – 12 месяцев со дня подписания договора.

Отчетный период – 3 календарных месяца.

Согласование документов проводится в не более чем 2 (две) итерации.

Документация согласовывается и передается в электронном виде в форматах \*.PDF и \*.DOCX.

Расширение или корректировка границ выполняемых работ закрепляется дополнительным соглашением сторон.

Гарантия на результаты работ – 12 месяцев. В течение указанного срока исполнителем оказывается сопровождение результатов работ: консультации или внесение изменений в случае поступления вопросов и замечаний со стороны регуляторов или ПАО «Сбербанк».

Перечень оказываемых Услуг приведен в таблице ниже.

Таблица 1 – Перечень оказываемых услуг

| № | Услуга | Ограничения |
| --- | --- | --- |
| 1 | Актуализация документации в рамках реализации требований 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в том числе при создании новых или модернизации существующих объектов КИИ, а также в случае изменения требований законодательства Российской Федерации | По заявкам |
| 2 | Разработка и актуализация иной технической документации при создании новых или модернизации существующих объектов КИИ (модели угроз, акты оценки соответствия и т.д.) | По заявкам |
| 3 | Участие в совещаниях рабочих групп и постоянно действующих комиссий по вопросам обеспечения безопасности КИИ и выполнения требований 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (дистанционно) | По заявкам |
| 4 | Анализ технических проектов и других документов на объекты КИИ с выдачей заключения о категории значимости и о необходимости принятия технических и организационных мер | По заявкам |
| 5 | Актуализация существующей проектной документации в части описания технических мер защиты информации | По заявкам |
| 6 | Подготовка предложений по модернизации системы защиты в соответствии с изменениями требований законодательства Российской Федерации | По заявкам |
| 7 | Оказание методической помощи в организации подготовки к проведению проверок со стороны контролирующих органов по вопросам защиты объектов КИИ, в том числе подготовка ответов (разъяснений) на поступившие Заказчику запросы и предписания | Без ограничений |
| 8 | Обучение эксплуатирующего объекты КИИ персонала Заказчика по вопросам ИБ/защиты КИИ | По заявкам |
| 9 | Оценка эффективности системы безопасности объектов КИИ | По заявкам |
| 10 | Иные консультационные вопросы по информационной безопасности | По заявкам |

* 1. Управление проектом

Исполнитель предоставляет Руководителя проекта, который обеспечивает единую «точку входа» для создания коммуникаций между Заказчиком и проектной командой. При реализации проекта Руководитель проекта и все участники проектной команды четко следуют требованиям выполнения работ в заданные сроки и с высоким качеством. Профессионализм участников проектных команд и полное соблюдение формализованных требований позволяет достичь высокого уровня оказываемых услуг. Главными критериями качества оказания услуг служит удовлетворенность Заказчика и сбалансированность ключевых показателей по сроку, бюджету и содержанию проекта.

* 1. Основные цели проекта

Необходимость проведения работ обусловлена требованиями Федеральных законов РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Целями Работ являются:

Выполнение требований законодательства РФ в области обеспечения безопасности объектов критической информационной инфраструктуры (КИИ).

Выбор оптимальной стратегии по приведению процессов обработки информации в соответствие с требованиями нормативно-правовых актов Российской Федерации, иным нормативно-правовым актам и национальным и отраслевым стандартам по защите информации, а также обеспечение должного уровня информационной безопасности (практическая безопасность).

* 1. Команда проекта

Перечень специалистов, требуемых для оказания услуг, приведен в таблице ниже. Указанный перечень является предварительным, по необходимости могут быть привлечены дополнительные специалисты по информационной безопасности (без изменения стоимости оказываемых услуг)

Таблица 2 – Перечень специалистов

| № | Тип исполнителя (должность, категория) | Количество |
| --- | --- | --- |
| 1 | Руководитель проекта (ГИП) | 1 |
| 2 | Ведущий консультант по защите информации | 1 |
| 3 | Консультант (аналитик) по защите информации | 1 |
| 4 | Аналитик по информационной безопасности (привлекается по необходимости) | 1 |
| 5 | Технический писатель  | 1 |
| Всего человек: | 5 |

* 1. Детализация оказываемых услуг

Общее количество часов по всем заявкам за 12 месяцев не должно превышать 280 ч. Расчетное количество часов по заявкам в течение отчетного периода (3 месяца) составляет 70 ч. В случае, если в течение отчетного периода (3 месяца) общая трудоемкость выполненных заявок составляет менее 70 ч., все неизрасходованные часы переносятся на следующие отчетные периоды в период действия договора, при этом оплата за отчетный период (3 месяца) производится в полном объеме. По согласованию с Исполнителем в течение отчетного периода могут быть израсходованы часы с последующих отчетных периодов. В таком случае оплата за отчетный период (3 месяца) производится в обычном объеме. При необходимости корректировка количества часов может быть оформлено дополнительным соглашением к договору.

* 1. Описание формата взаимодействия
* Исполнитель должен обеспечивать возможность регистрации заявок (обращений) Заказчика по следующим каналам связи:
* электронная почта;
* телефонная связь (номер 8800 или иная технология, обеспечивающая бесплатные для Заказчика обращения посредством звонков);
* информационная система типа service desk:
* иные каналы коммуникации (по согласованию сторон).

Все заявки и их результаты фиксируются Исполнителем в Журнале учета заявок (в электронной форме). После регистрации заявки Исполнитель по электронной почте согласовывает с Заказчиком расчетную трудоемкость (для заявок, трудоемкость которых превышает 48 часов) и срок исполнения заявки и затем приступает к выполнению заявки. В случае срочных (критичных) заявок Исполнитель может приступить к выполнению до получения согласований со стороны Заказчика.

Работы выполняются дистанционно, необходимость очных работ согласовывается сторонами по факту возникновения такой необходимости.

1. Основные цели оказания услуг:
* минимизация затрат Заказчика и выбор оптимальной стратегии приведения в полное соответствие требованиям нормативно-правовых актов Российской Федерации (НПА РФ) и руководящих документов ФСТЭК России и ФСБ России в области защиты информации;
* минимизация рисков информационной безопасности, срабатывание которых может повлечь нарушение функционирования объектов защиты и негативные экономические, социальные, экологические, политические последствия и иные виды последствий;
* построение комплексной системы защиты информации, обеспечивающей нейтрализацию угроз безопасности информации, в соответствии с НПА РФ и лучшими международными практиками;
* построение системы менеджмента информационной безопасности (СМИБ), обеспечивающей внедрение и поддержание процессов информационной безопасности на всех стадиях жизненного цикла объектов КИИ;
* успешное прохождение проверок регулирующими органами (ФСТЭК России, Прокуратура РФ).

Для достижения обозначенных целей необходимо выполнить следующие работы:

* обследование информационной инфраструктуры: архитектуры информационных систем (ИС), информационно-телекоммуникационных сетей (ИТС), автоматизированных систем управления технологическими процессами (АСУ ТП); комплекса технических средств; каналов связи;
* сбор сведений об обрабатываемой конфиденциальной информации; информационных потоках; пользователях; ролях и правах доступа к информации и техническим средствам;
* обследование существующих организационных и технических мер по обеспечению защиты информации;
* оценка рисков;
* оценка соответствия принятых организационных и технических мер требованиям НПА РФ по обеспечению защиты информации и (или) лучшим международным практикам;
* разработка Моделей угроз и нарушителя безопасности информации объектах КИИ с применением методологии Kill Chain;
* формирование требований к системе защиты информации и разработка технического задания на создание системы защиты информации;
* эскизное проектирование системы защиты информации;
* стендовые испытания средств защиты информации (при необходимости);
* технорабочее проектирование системы защиты информации и поставка средств защиты информации;
* разработка эксплуатационной документации на систему защиты информации;
* разработка организационно-распорядительных документов (ОРД) по обеспечению информационной безопасности с применением процессной модели и цикла Деминга (Plan - планируй, Do - выполняй, Check - проверяй, Act – действуй; PDCA);
* пусконаладочные работы по вводу в действие системы защиты информации;
* тестирование на проникновение и (или) анализ защищенности объекта защиты в процессе опытной эксплуатации;
* внесение изменений в конфигурацию средств защиты по результатам тестирования на проникновение и (или) анализа защищенности, и приемка системы защиты информации в постоянную эксплуатацию;
* оценка соответствия средств защиты информации в составе системы защиты информации, в том числе встроенных в программные и (или) программно-аппаратные средства ЗОКИИ;
* сопровождение системы защиты информации на всех стадиях жизненного цикла.

Принципы, которыми должен руководствоваться Исполнитель при оказании услуг:

* минимизация затрат Заказчика;
* выполнение всех работ в заданные сроки;
* в основе подходов – национальные стандарты РФ и лучшие международные практики в части, не противоречащей НПА РФ;
* привлечение на проект сертифицированных и (или) профильных специалистов;
* нацеленность на применение существующих (применяемых) у Заказчика технических и организационных мер защиты объектов КИИ;
* подходы, нацеленные на непрерывность бизнеса.

1. Услуги по защите конфиденциальной информации

Создание системы защиты информации (далее – СЗ) – это сложный многоуровневый процесс, затрагивающий оптимизацию бизнес-процессов организации, внедрение технических средств защиты информации, а также эффективное организационное управление информационной безопасностью.

Исходя из этого, проект предполагается реализовывать в несколько последовательных этапов

* 1. Обследование

Работы по защите конфиденциальной информации (далее – КИ) начинаются с обследования технологических процессов обработки КИ, составления целостной картины об IT-инфраструктуре Заказчика и анализа применяемых организационных и технических мер обеспечения безопасности КИ.

Целью данного этапа является оценка обстановки и выбор на ее основе оптимальной стратегии обеспечения безопасности КИ.

Задачи этапа:

* анализ технологических процессов обработки КИ, включая неавтоматизированную обработку;
* обследование информационной инфраструктуры: архитектуры информационных систем (ИС), информационно-телекоммуникационных сетей (ИТС), автоматизированных систем управления технологическими процессами (АСУ ТП); комплекса технических средств; каналов связи;
* сбор сведений об информационных потоках; пользователях; ролях и правах доступа к информации и техническим средствам;
* разработка перечня КИ, обрабатываемых в организации, а также перечня подразделений и работников, допущенных к такой обработке;
* юридический анализ внутренних документов на предмет соответствия законодательству о КИ;
* оценка состояния обеспечения безопасности КИ;
* разработка рекомендаций по оптимизации бизнес-процессов обработки КИ;
* классификация КИ в соответствии с нормативно-правовыми актами РФ.

* 1. Категорирование объектов КИИ (при необходимости)

В случае необходимости проведения работ по категорированию объекта критической информационной инфраструктуры в обязательном порядке разрабатывается документ «Методика категорирования объектов КИИ», в зависимости от особенностей функционирования объектов КИИ, технологических и бизнес-процессов. Методика категорирования может разрабатываться с учетом временных интервалов (SLA), полученных на этапе оценки рисков.

Методы оценки рисков используются как вспомогательные в отношении объектов КИИ, которые автоматизируют процессы на опасном производственном объекте (ОПО) или объекте топливно-энергетического комплекса (ТЭК). В этом случае категорирование осуществляется на основании деклараций промышленной безопасности, планов ликвидации последствий аварий и паспортов объектов

* 1. ТЭК и ОПО.

Целью данного этапа является оценка значений показателей уровня значимости в соответствии с Постановлением 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».

Задачи этапа:

* анализ полученных данных на этапе обследования;
* разработка Методики категорирования;
* определение актуальных нарушителей безопасности информации;
* идентификация ключевых угроз безопасности информации;
* подготовка документов для отправки во ФСТЭК России;
* согласование документов со ФСТЭК России (внесение изменений при необходимости).

Результатом работ по этапу «Категорирование» должны являться:

Методика категорирования объектов КИИ.

Акт категорирования объектов КИИ.

Формы направления сведений в соответствии с Приказом ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

* 1. Моделирование угроз

Для выполнения требований законодательства о защите КИ Заказчику необходимо применять организационные и технические меры для защиты КИ от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения КИ, а также от иных неправомерных действий.

Целью данного этапа является оценка подверженности ИС/АСУ/ИТС, обрабатываемых КИ, кибератакам и описание возможных векторов атак.

Атака на ИС/АСУ/ИТС представляет собой последовательно реализованные угрозы безопасности информации (цепочку атаки, от англ. Kill Chain).

В основе подхода набор самых распространенных типов (видов) кибератак, составленных с учетом техник, описанных в OWASP Top 10 (Open Web Application Security Project), CAPEC (Common Attack Pattern Enumeration and Classification) и MITRE ATT&CK.

В Модели угроз рассматриваются цепочки возможных атак на ИС/АСУ/ИТС, состоящие из угроз безопасности информации (далее – УБИ), согласно принятой в Банке данных угроз ФСТЭК России (https://bdu.fstec.ru/) классификации и обозначениям.

Задачи этапа:

* определение актуальных нарушителей безопасности КИ путем анализа определенных критериев, свойственных для филиала и юр. лица Заказчика в целом;
* определение объектов воздействия (серверы, автоматизированные рабочие места пользователей, системное и прикладное программное обеспечение, аппаратные платформы, активное сетевое оборудование, машинные носители и т. п.) в зависимости от структурно-функциональных характеристик (архитектуры) ИС/АСУ/ИТС;
* выборка применимых УБИ из Банка данных угроз ФСТЭК России в зависимости от особенностей объектов воздействия (опционально могут быть рассмотрены дополнительные угрозы, предусмотренные национальными стандартами и лучшими практиками в области обеспечения информационной безопасности);
* составление цепочек атак (Kill Chain) из выборки применимых УБИ;
* расчет вероятности реализации УБИ с учетом реализованных организационных мер защиты и потенциала нарушителя безопасности КИ (на данном этапе не учитываются реализованные технические меры защиты информации с целью полного документирования и комплектования создаваемой СЗ, за исключением случаев модернизации существующей СЗ с ранее выданным аттестатом соответствия или заключения о прохождении процедуры оценки соответствия);
* формирование итогового перечня актуальных УБИ;
* адаптация, уточнение и дополнение мер, необходимых для нейтрализации актуальных УБИ;
* формирование итогового перечня организационных и технических мер, необходимых для нейтрализации актуальных УБИ.

Результатом работ по этапу «Моделирование угроз» будут являться частные Модели угроз для каждой ИС/АСУ/ИТС, обрабатываемой КИ. При необходимости разработанные Модели угроз проходят согласование со ФСТЭК России и ФСБ России.

* 1. Формирование требований к СЗ

Целью данного этапа является детализация итогового перечня мер, полученного на предыдущем этапе, и разработка Технического задания на создание (модернизацию) СЗ в соответствии с требованиями руководящих документов ФСТЭК России и ФСБ России, содержащего:

* назначение и цели создания СЗ;
* состав подсистем СЗ и требования к ним;
* требования к режимам функционирования СЗ;
* требования к составу и содержанию работ по подготовке объекта автоматизации к вводу СЗ в действие;
* состав и содержание работ по созданию СЗ;
* порядок контроля и приемки СЗ;
* требования к персоналу;
* требования к документированию.

При необходимости разработанное Техническое задание на создание (модернизацию) СЗ проходит согласование со ФСТЭК России.

* 1. Эскизное проектирование СЗ

Целью данного этапа является подбор и описание необходимых функций средств защиты информации, входящих в состав СЗ, с целью бюджетирования закупки и последующего внедрения в ИТ-инфраструктуру Заказчика.

Типовой комплект документации эскизного технического проекта включает в себя следующие документы:

* Схема структурная комплекса технических средств,
* Спецификация (ведомость покупных изделий).
* Стендовые испытания СЗ

Данный этап необходим для подтверждения совместимости проектируемых решений и исключения негативного воздействия на функционирование объектов КИИ. Работы проводятся совместно с Вендором.

* 1. Технорабочее проектирование СЗ

Целью данного этапа является разработка технорабочего проекта и детальное описание конфигурации средств защиты информации и вносимых изменений в ИТ-инфраструктуру Заказчика.

* Типовой комплект технорабочей документации включает в себя следующие документы:
* Ведомость технорабочего проекта на создание (модернизацию) СЗ;
* Пояснительная записка к технорабочему проекту;
* Описание комплекса технических средств;
* План производства работ;
* Таблица соединений и подключений;
* Программа и методики испытаний;
* План серверных помещений и расположения оборудования в серверных стойках;
* Эксплуатационная документация СЗ (инструкции операторов, администраторов, регламент аварийного восстановления и технического обслуживания, регламент резервного копирования и т.п.).

Результатом работ по этапу «Технорабочее проектирование СЗ» будет являться комплект документации технорабочего проекта, описанный выше.

* 1. Разработка ОРД

Целью данного этапа является формирование комплекта организационно-распорядительной документации, позволяющего привести процессы обработки КИ, в том числе эксплуатации средств криптографической защиты информации в соответствие с требованиями российского законодательства и руководящих документов ФСТЭК России и ФСБ России.

Должен быть разработан типовой комплект документов с учетом процессного подхода, обладающий следующими преимуществами:

Структурированный комплект документов, основанный на процессном подходе и цикле Деминга (Plan, Do, Check, Act – PDCA).

В основе документов – требования НПА РФ в области защиты информации, национальные стандарты РФ, стандарты серии ISO, NIST Cybersecurity Framework, методические документы ФСТЭК и ФСБ России, лучшие практики от производителей ПО и оборудования, например, Cisco Safe Best Practice.

Типовая структура верхнеуровневых документов упрощает поддержание их в актуальном состоянии.

Наличие ролей и ответственных за процессы.

Описание и расчет трудозатрат на внедрение и поддержание процессов.

Возможность интеграции процессов, описанных в документах, в систему электронного документооборота.

Возможность адаптации документов под конкретную штатно-организационную структуру и информационную инфраструктуру.

Возможность интегрировать в документы различные требования, например, по защите ПДн, ГИС, КТ и других видов тайн.

Описанные в ОРД процессы должны быть интегрированны в систему электронного документооборота.

* 1. Комплектация, поставка и ввод в действие СЗ

В соответствии с разработанным Техническим заданием на создание (модернизацию) СЗ и технорабочим проектом, проводятся работы по вводу в действие СЗ.

На данном этапе специалисты Исполнителя решают следующие задачи:

* пилотирование средств защиты информации (при необходимости);
* поставка средств защиты информации;
* разработка рабочей документации в составе: план пуско-наладочных работ; таблица соединений и подключений; программа и методика испытаний (предварительных/опытных); протоколы испытаний, акты о переводе СЗ в опытную и постоянную эксплуатации; руководство пользователя СЗ; руководство администратора СЗ;
* монтаж и настройка средств защиты информации;
* проведение приемо-сдаточных испытаний.

Результатом работ на этом этапе является сданная в опытную эксплуатацию СЗ.

* 1. Анализ защищенности или тестирование на проникновение

В ходе опытной эксплуатации СЗ необходимо провести инструментальный анализ защищенности или тестирование на проникновение, чтобы убедиться, что вновь созданная СЗ, а также выработанные организационные и технические меры, нейтрализуют все УБИ, выявленные на этапе моделирования угроз.

Тестирование на проникновение проводится с учетом Модели нарушителя, разработанной на предыдущих этапах, и осуществляется в несколько этапов:

внешнее тестирование;

внутреннее тестирование;

социотехническое тестирование.

В зависимости от Модели нарушителя, тестирование может проводиться методами «черного» или «белого» ящиков.

В случае если в ходе анализа защищенности или тестирования на проникновение будут обнаружены актуальные УБИ и уязвимости – вносятся изменения в конфигурацию средств защиты информации или выполняется обновление программного обеспечения, в том числе СЗ.

При отсутствии уязвимостей проводятся приемочные испытания и СЗ сдается в постоянную эксплуатацию.

* 1. Аттестация

Аттестация ­­– это процедура оценки соответствия объекта информатизации предъявляемым требованиям законодательства. Аттестация по требованиям безопасности обязательна для государственных информационных систем и в ряде других случаев.

В ходе аттестационных испытаний комиссией из работников компании-лицензиата ФСТЭК России проводится тщательная оценка соответствия организационных и технических мер, включая испытания СЗ. По итогам процедуры выдается аттестат, подтверждающий соответствие требованиям, предъявляемым для обеспечения безопасности соответствующей категории защищаемой информации.

Наличие аттестата позволяет:

подтвердить соответствие системы требованиям конкретного законодательства;

снизить риски при прохождении проверок со стороны регуляторов;

повысить имидж и уровень доверия к компании на рынке (в случае предоставления услуг партнерам или физическим лицам).

* 1. Сопровождение СЗ в ходе эксплуатации

В процессе эксплуатации СЗ могут возникнуть предпосылки для ее доработки. Например, при необходимости пересмотра классификации КИ, в результате предписаний контрольно-надзорных органов по итогам проверок и пр. Наша компания обеспечит сервисную и консультационную поддержку режима защиты объекта информатизации на безопасном уровне в соответствии с законодательством Российской Федерации.

В ходе оказания сервисной поддержки предполагается (на выбор или в комплексе):

проведение аудитов с целью контроля и анализа вносимых в СЗ изменений на предмет соответствия требованиям законодательства РФ о защите информации;

консультирование по вопросам обеспечения безопасности КИ;

сопровождение программных и (или) программно-аппаратных средств защиты информации;

сопровождение при проведении проверок контрольно-надзорных органов в сфере защиты КИ;

повышение осведомленности персонала по вопросам информационной безопасности;

ежегодный контроль эффективности реализованных организационных и технических мер защиты КИ;

анализ защищенности в формате Red Team (24/7).

1. Заключительные требования

Работы должны проводиться в соответствии с учетом требований российского законодательства и руководящих документов ФСТЭК России и ФСБ России. Все работы должны проводиться компетентными специалистами, имеющими опыт оказания услуг по защите конфиденциальной информации, анализа технологических процессов (бизнес-процессов), проведения аттестаций объектов информатизации.

При оказании услуг должны применяться методики, основанные как на обязательных требованиях законодательства Российской Федерации (ФСТЭК и ФСБ России, Роскомнадзор, Минсвязи), так и на лучших международных практиках (ISO, NIST, COBIT, ITIL, PMBOK).

В составе проектной группы Исполнителя должны присутствовать профильные специалисты с опытом работы в области информационной безопасности от 5 до 12 лет и высшим образованием по направлению «Информационная безопасность», а также прошедшие обучение на специализированных курсах, включая «Certificate Ethical Hacker», «Computer Hacking Forensic Investigator», «Ethical Hacking», курсов по сканерам защищенности (MaxPatrol, Qualys и т.п.) и другим средствам защиты информации.

Исполнительдолжен обладать лицензиями на:

Деятельность по технической защите конфиденциальной информаии

Деятельность по разработке и производству средств защиты конфиденциальной информации

Осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств