ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке № 271578, Работы по разработке Стратегии развития информационной безопасности компании способом «Открытый тендер на понижение»

Лот № 858042

Заказчик: Акционерное общество "Национальная атомная компания "Казатомпром"

Организатор: Акционерное общество "Национальная атомная компания "Казатомпром"

1. **Краткое описание ТРУ**

Наименование	**Значение**
Номер строки	27 Р
Наименование и краткая характеристика	Работы по разработке политики/стратегии компании, Работы по разработке политики/стратегии компании
Дополнительная характеристика	Работы по разработке Стратегии развития информационной безопасности АО "НАК "Казатомпром"
Количество	1
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, ул. Е-10 д. 17/12
Условия поставки	-
Срок поставки	С даты подписания договора в течение 120 календерных дней
Условия оплаты	Окончательный платеж - 100%, Промежуточный платеж - 0%, Предоплата - 0%

2. **Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики**

Глава 1. Общие положения

1.Руководство АО «НАК «Казатомпром» (далее - Компания), учитывая, что киберриски стали фундаментальным риском для основного бизнеса Компании, приняло решение о разработке «Стратегии Информационной Безопасности» (далее - Стратегия).

2.Стратегия разрабатывается сроком на 5 лет.

3.Основными целями разработки Стратегии является;

1)Целевая архитектура ИБ (кибербезопасности);

2)Актуализация процесса обеспечения ИБ в Компании для максимально эффективного снижения рисков целевых кибератак и их последствий;

3)Разработка метрик эффективности обеспечения ИБ (кибербезопасности);

4)Гармонизация задач по обеспечению ИБ (кибербезопасности) со Стратегией развития Компании и другими внутренними документами в области Цифровизации и ИТ.

4.Для достижения поставленной цели, Стратегия должна содержать:

1)Анализ текущей ситуации обеспечения ИБ в Компании в разрезе следующих направлений:

a.Руководство информационной безопасностью;

b.Организационная структура, навыки и компетенции

c.Управление рисками информационной безопасностью;

d.Управление непрерывностью бизнеса;

e.Процессы (операционная модель) и используемые инструменты;

f.Соответствие требованиям законодательства.

2)Анализ возможных типов, векторов и целей кибератак;

3)Оценка / данные из международной практики в части киберугроз для предприятий атомной промышленности;

4)Перечень стратегических целей, задач по информационной безопасности (кибербезопасности);

5)Способы достижения поставленных задач в разрезе направлений п.1;

6)Расчетные показатели выполнения поставленных задач;

7)Перечень возможных рисков реализации задач;

8)Определение операционной модели обеспечения ИБ (кибербезопасности) по следующим функциональным областям:

a.Руководство и контроль;

b.Управление рисками ИБ (кибербезопасности);

c.Управление уязвимостями и угрозами (анализ угроз, тестирование на проникновение);

d.Резервирование и восстановление (непрерывность бизнеса)

e.Мониторинг ИБ и отчетность;

f. Управление архитектурой ИБ и изменениями;

g.Управление идентификацией и доступом;

h.Сорсинг и управление поставщиками;

9)Принципы организационной структуры ИБ (кибербезопасности);

10)Целевая архитектура ИБ;

11)План и этапы реализации стратегических задач;

5.Термины и сокращения, используемые в документе:

Компания/ Заказчик – Акционерное общество «Национальная атомная компания «Казатомпром»;

Подрядчик – Юридическое лицо, определенное победителем по итогам проведенных закупок в соответствии с Правилами закупок товаров, работ и услуг АО «Самрук-Қазына»;

Проект – Разработка «Стратегии развития ИБ» Компании в среднесрочной перспективе, в соответствии со «Стратегическим планом Развития» Компании;

ДБ – Департамент безопасности;

ДПИТ – Департамент поддержки информационных технологий;

ДО – Дочерние организации;

Договор – Договор закупок работ по разработке Стратегии;

ИБ – Информационная безопасность;

КБ – Кибербезопасность;

ИТ – Информационные технологии;

ИБ-проект – Разработка и внедрение систем(ы) ИБ;

ИБ-процесс – Процесс обеспечения ИБ (Защита информационных систем и активов от кибератак);

ИБ-услуги – Комплекс работ, направленный на поддержание процесса обеспечения ИБ;

ПО – Программное обеспечение;

СТ РК – Система стандартизации Республики Казахстан;

Стратегия – Стратегии развития ИБ;

СУИБ – Система управления информационной безопасностью;

ТО – Техническое обоснование;

ТС – Техническая спецификация;

ТЭО – Технико-экономическое обоснование;

ENISA – Рекомендации в области кибербезопасности
(The European Union Agency for Network and Information Security);

ISO/ IEC 27000– Группа международных стандартов в области обеспечения ИБ;

Kill Chain – «Убийственная цепочка» - военный термин, адаптированный компанией Lockheed Martin к области информационной безопасности как модель, отражающая последовательность действий потенциального злоумышленника от этапа «разведки» (обнаружения потенциальных уязвимостей) до совершения действий в компьютерной сети организации по разрушению активов организации;

NCSC – Рекомендации в области кибербезопасности
(National Cyber Security Centre / UK);

NIST (Cybersecurity) – Рекомендации в области кибербезопасности
(National Institute of Standards and Technology / US. Department of Commerce);

NRC – Требования по кибербезопасности для атомных станций
/ Nuclear Power Plant Cyber Security: Highly Controlled, Fully Protected
(Nuclear Regulatory Commission / US)

Глава 2. Временные требования при разработке Стратегии

6.Стратегия разрабатывается сроком на 5 лет.

7.Сроки выполнения:

1)Общий срок разработки Стратегии не должен превышать 120 календарных дней с даты подписания договора о

закупках;

2)В течение 10 рабочих дней с даты начала работ, должны быть согласованы:

•Устав Проекта;

•График работ.

8.Этапы Проекта. Проект делится на 4 части:

1)Обследование и интервью с руководителями ключевых подразделений Компании;

2)Разработка Стратегии и сопутствующих документов;

3)Согласование Стратегии с подразделением ИБ Компании;

4)Подготовка итоговой презентации для Руководства Компании.

9.Все работы проводятся в головном офисе Компании или удаленно, по согласованию с Руководителем Проекта.

10.Разработка Стратегии считается завершенной в момент подписания акта приема-передачи разработанной Стратегии и сопутствующих документов Заказчику.

Глава 3. Требования по содержанию Стратегии

11.Стратегия должна учитывать:

a.Законодательные и нормативные требования РК в области ИБ и кибербезопасности;

b.Рекомендации Фонда «Самрук-Казына» в области ИБ;

c.Стратегия развития АО «НАК «Казатомпром» на 2018-2028 годы;

d.Стратегия развития ИТ АО «НАК «Казатомпром» на 2018-2028 годы;

e.Международные отраслевые требования и рекомендации в области ИБ и кибербезопасности (NIST, ENISA, ISO/IEC).

12.Стратегия должна обязательно содержать следующие разделы

1)Вводные данные о Компании и ее стратегическом развитии;

2)Анализ текущей ситуации по обеспечению ИБ в Компании:

•Анализ угроз на основе процесса Kill Chain,

•Перечень рисков,

•Экспертная оценка из значимости;

3)Анализ возможных векторов кибератак:

•Перечень и анализ реальных случаев целевых кибератак на промышленные объекты,

•Перечень возможных векторов кибератак с учетом изменения технологического ландшафта Компании;

4)Оценка / данные из международной практики в части киберугроз для предприятий атомной промышленности:

•Сравнение данных из открытых источников по отрасли;

5)Перечень стратегических задач по кибербезопасности;

6)Перечень возможных рисков при реализации задач;

7)Расчетные показатели выполнения поставленных задач;

8)Определение операционной модели обеспечения ИБ и принципов организационной структуры;

9)Целевая архитектура ИБ, охватывающая следующие области:

•IT Infrastructure Security,

•OT Infrastructure Security,

•Data Protection,

•Network Security,

•Перечень и описание использованных моделей;

13.Отдельно разрабатывается План мероприятий по реализации Стратегии, содержащий планы и этапы реализации стратегических задач;

14.Комплект документов, который должен появиться по завершению разработки:

1)«Стратегия Информационной Безопасности».

2)Актуализированная «Политика информационной безопасности».

3)«Ландшафт киберугроз и возможных сценариев кибератак для предприятий атомной энергетики».

4)«Свод нормативных требований и отраслевых рекомендаций».

5)«Целевая Архитектура ИБ».

6)«План мероприятий по реализации Стратегии».

7)«Аналитический отчет с информацией полученной в ходе обследования ключевых подразделений Компании».

8)Итоговая презентация по проекту.

Глава 4. Состав проектной группы

15.Руководство и состав участников проекта:

a.Руководитель проекта – представитель Подрядчика.

b.Менеджер проекта - ответственный работник подразделения ИБ.

c.Архитектор проекта (Главный Разработчик Стратегии) - представитель Подрядчика, ответственный за разработку Стратегии.

d.Эксперты по направлениям – представители Подрядчика, привлекаемые Архитектором Проекта, для реализации тех или иных специфичных задач.

Глава 5. Требования к Подрядчику (работникам Подрядчика).

16.Требования к членам проектной команды Подрядчика:

a.Наличие у руководителя проекта сертификатов в области проектного управления (PMP, IPMI, IPMA, CompTIA IT Project+);

b.Наличие в команде не менее трех членов, обладающих квалификациями в области информационной безопасности,

подтверждаемых соответствующими международными сертификатами (CISM, CISSP, Security+, СУИБ ISO 27001 lead implementer).

c.Наличие в команде не менее одного члена команды, обладающего квалификациями в области информационной безопасности, подтверждаемых соответствующими международными сертификатами (CompTIA CySA+, EC Council Certified Network Defender, Cisco CCNA Cyber Ops, CCNA Security, CCNP Security).

d.Наличие в команде не менее одного члена команды, обладающего квалификациями в области информационной безопасности АСУТП, подтверждаемых соответствующими международными сертификатами (Certified SCADA Security Architect (CSSA), GIAC ICS Security Professional (GICSP) ICS CERT VLP 210-W Cybersecurity for ICS).