Құжат «Самұрық-Қазына» ӘАҚ» АҚ электронды порталымен құрылған
Документ сформирован порталом электронных закупок АО «ФНБ «Самрук-Казына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 494884
способом Открытый тендер на понижение

Лот № (40-4 У, 1753346) Услуги по проведению аудита информационных технологий

Заказчик: Акционерное общество "Самрук-Энерго"
Организатор: Акционерное общество "Самрук-Энерго"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	40-4 У
Наименование и краткая характеристика	Услуги по проведению аудита информационных технологий, Услуги по проведению аудита информационных технологий
Дополнительная характеристика	Аудит систем информационной безопасности, разработка организационно-распорядительной документации по информационной безопасности
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Нур-Султан, пр.Кабанбай Батыра 15А, Блок Б
Условия поставки	-
Срок поставки	С даты подписания договора в течение 30 рабочих дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

Код ЕНС ТРУ 749020.000.000072

1 Предмет закупки
Услуги по проведению аудита информационных технологий
2 Объем услуг
Таблица 1. Перечень услуг
№
п/п Описание и требуемые технические и качественные характеристики услуг Ед.
изм. Кол-во Сроки оказания/выполнения
(при наличии)
1 2 3 4 5
1 Внешняя независимая оценка эффективности контролей, подтверждающая защищенность программ и систем Компании от кибер-рисков Услуга 1 С даты заключения договора в течении 30 рабочих дней

3 Список используемых сокращений и терминов:

Сокращение Определение сокращения
ВНД Внутренний нормативный документ
ДБ Департамент «Безопасность»
Заказчик АО «Самрук-Энерго»
Исполнитель Поставщик услуг, с которым Заказчик заключил договор на оказание Услуги
Инфраструктура ИТ/ИБ Программные и аппаратные средства, корпоративные данные и информация в электронном виде, обеспечивающие работу сервисов ИТ/ИБ, используемых Заказчиком
ИС Информационная система
ИБ Информационная безопасность
Сервисы ИБ Комплекс ИБ-решений и деятельности, обеспечивающий реализацию информационной безопасности Заказчика
СУИБ Система управления информационной безопасности
Оборудование Аппаратные средства, передаваемые Заказчиком на обследование Исполнителю
ОС Операционная система
ПО Программное обеспечение
ТС Техническая спецификация
Услуга Внешняя независимая оценка эффективности контролей, подтверждающая защищенность программ и систем Компании от кибер-рисков

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе

4 Общие сведения

Обследование должно представлять собой независимое исследование, направленное на получение качественных и объективных результатов. Для выполнения услуг по обследованию Исполнитель создает группу специалистов, имеющих соответствующее профессиональное образование и практический опыт работы в соответствующих отраслях. В ходе оказания услуг должны учитываться требования и рекомендации следующих нормативных актов и стандартов:

• СТ РК ИСО/МЭК 27002-2015. Методы обеспечения защиты. Свод правил по управлению защитой информации.
• СТ РК ИСО/МЭК 27001-2015. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
• Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V.
• Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V.
• Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».
• Иные нормативно-правовые документы РК в области информационных технологий и их защиты.
• ISA099/IEC-62443. Security for Industrial Automation and Control Systems;
• GDPR. General Data Protection Regulation;
• NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security;
• NERC. Critical Infrastructure Protection.

5 Требования к оказанию услуг

Основная цель – оценка текущего уровня защищенности ИТ/ИБ инфраструктуры и разработка рекомендаций по реализации комплекса организационных и технических мер, направленных на защиту ИС АО «Самрук Энерго», а также рекомендации на соответствие требованиям информационной безопасности по международному стандарту ISO 27001.

Для достижения поставленной цели в ходе оказания услуг должны быть решены следующие задачи:

• Анализ существующей ситуации оснащенности ИТ инфраструктуры;
• Анализ существующего состояния ИС;
• Анализ существующего состояния организационного и технического уровня обеспечения ИБ;
• Выработка соответствующих рекомендаций по повышению осведомленности в области СУИБ обслуживающего персонала Заказчика;
• Инструментальное обследование на уязвимости;
• Разработка рекомендаций по развитию ИТ инфраструктуры;
• Разработка рекомендаций по техническому дооснащению средствами обеспечения ИБ;
• Разработка рекомендаций по устранению и минимизации ошибок, рисков и уязвимостей;
• Разработка рекомендаций по составу и содержанию необходимых организационных и технических мер обеспечения безопасности информации, направленных на повышение уровня ИБ, включая разработку и актуализацию следующей ВНД по ИБ, согласно СТ РК ИСО/МЭК 27002-2015, СТ РК ИСО/МЭК 27001-2015:

политика информационной безопасности;
правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;
методика оценки рисков информационной безопасности;
правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;
правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;
правила проведения внутреннего аудита информационной безопасности;
правила использования криптографических средств защиты информации;
правила разграничения прав доступа к электронным ресурсам;
правил использования Интернет и электронной почты;
правила организации процедуры аутентификации;
правила организации антивирусного контроля;
правила использования мобильных устройств и носителей информации;
правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов;
регламент резервного копирования и восстановления информации;
инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях.

6 Границы проведения услуг

6.1 Состав обследуемых организационных, технических и программных средств АО «Самрук-Энерго»:

• все прикладное ПО;
• активное сетевое оборудование (коммутаторы, маршрутизаторы, межсетевые экраны): этажные маршрутизаторы, межсетевые экраны;
• физические сервера;
• виртуальные сервера;
• базы данных;
• серверные операционные системы;

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе

• системы хранения данных;
• физические ПК пользователей;
• действующая ВНД по СУИБ.
6.2 В область проведения аудита должны входить:
• технические средства, обеспечивающие автоматизацию управления процессами;
• сеть передачи данных, обеспечивающая взаимодействие технических средств ИС;
• сети/сегменты взаимодействия сетей Прикладных систем и корпоративной сети Заказчика;
• программное обеспечение ИС в части анализа конфигурации встроенных средств безопасности и анализа на наличие уязвимостей;
• ВНД Заказчика, устанавливающая требования в части обеспечения ИБ;
• эксплуатационная документация Прикладных систем;
• используемые специализированные средства защиты информации в сетях передачи данных;
• персонал, обеспечивающий эксплуатацию ИС и ее информационную безопасность.
6.3 Обследование внешнего сетевого периметра - проведение внешнего сканирования сетевого периметра на наличие известных уязвимостей.
6.4 Методология выполнения услуг и перечень инструментальных проверок должны быть определены Исполнителем по согласованию с Заказчиком на этапе инициализации аудита (детализации плана-графика оказания услуг).

7 Этапы оказания услуг
Этап 1. Комплексное обследование ИТ инфраструктуры.

На основании результатов комплексного обследование ИТ инфраструктуры и технических средств обеспечения ИБ в АО «Самрук-Энерго» должны быть выявлены существующие уязвимости в инфраструктуре, приводятся рекомендации по их устранению, разрабатывается и согласовывается календарный план оказания услуг, а также производится расчёт затрат на модернизацию ИТ инфраструктуры.

№ Наименование услуг Описание
1 Обследование сетевой инфраструктуры В состав услуг входят:
- обследование архитектуры построения сети передачи данных;
- анализ конфигурационных файлов сетевых устройств;
- анализ топологии сети, состава и характеристик программных и аппаратных средств;
- создание существующей физической и логической схем сети;
- инвентаризация сетевого оборудования;
- описание текущего состояния;
- выработка рекомендаций по устранению недостатков;
- проведение внутреннего сканирования сети на наличие известных уязвимостей.
2 Оценка рисков информационной безопасности В состав услуг входят:
- аудит информационной безопасности на предмет определения актуальных рисков информационной безопасности организации (идентификация и классификация информационных ресурсов по степени их критичности, определение уровня защищенности информационных ресурсов и активов)
- анализ рисков информационной безопасности (количественная и качественная оценка степени ущерба от реализации угроз с учетом их возможности);
- оценка вероятности их реализации и возможного ущерба.
3 Обследование конечных устройств В состав услуг входят:
- обследование аппаратной части;
- обследование программной части;
- выборочная инвентаризация рабочих станций;
- обследование политик безопасности;
- сканирование рабочих станций на наличие уязвимостей.
Количество обследованных устройств должно быть обоснованным и достаточным для вынесения решения о состоянии конечных устройств.
4 Обследование беспроводного сегмента сети В состав услуг входят:
- обследование архитектуры построения беспроводного сегмента сети;
- анализ конфигурационных файлов устройств;
- обследования оборудования беспроводной сети;
- инвентаризация оборудования беспроводной сети;
- описание текущего состояния;
- выработка рекомендаций по устранению недостатков.
5 Обследование системы телефонии, видеоконференцсвязи В состав услуг входят:
- обследование оборудования внутренних коммуникаций (телефония, видеоконференцсвязь);
- инвентаризация оборудования внутренних коммуникаций;
- описание текущего состояния сегмента внутренних коммуникаций;
- выработка рекомендаций по устранению недостатков.
6 Обследование внешнего сетевого периметра В состав услуг входят:
- обследование оборудования внешнего сетевого периметра;

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе

- анализ конфигурационных файлов оборудования;
- описание текущего состояния;
- выработка рекомендаций по устранению недостатков.
7 Обследование центра обработки данных В состав услуг входят:
- обследование физической организации и инженерных систем;
- обследование программной части выборочных серверов;
- обследование аппаратной части выборочных серверов;
- обследование систем хранения данных;
8 Обследование приложений В состав услуг входят:
- обследование службы каталогов;
- обследование службы доставки электронной почты;
- обследование Прикладного ПО.
9 Обследование технических средств обеспечения ИБ В состав услуг входят:
- обследование средств обеспечения ИБ;
- анализ эффективности внедренных программно-технических средств.
10 Модернизация ИТ и ИБ инфраструктуры В состав услуг входят:
- составление рекомендаций и/или технического задания на модернизацию ИТ/ИБ инфраструктуры.
11 Проверка на соответствие требованиям В состав услуг входят:
Проверка предприятия на соответвие требования стандарта ISO/IEC 27001 и выдача рекомендаций и регламента по защите данных GDPR – General Data Protection Regulation.

По итогам проведенного обследования предоставляются следующие документы:
• Резюме, содержащее краткие итоги оказанных услуг;
• Отчет с оценкой текущего состояния ИТ инфраструктуры, с учетом требований информационной безопасности, включающий в себя: описание каждого элемента ИТ инфраструктуры, технологическую модель ИТ инфраструктуры (реализованную и рекомендуемую), отчет о выявленных уязвимостях, рекомендации по их устранению и бюджетную оценку;

Этап 2. Рекомендации по внедрению СУИБ

На основании консультационно-методических мероприятий по внедрению СУИБ необходимо обследование текущей ВНД, и выдача рекомендаций по исправлению и/или использованию действующих документов.
1. Первичные организационные мероприятия в состав услуг входит:
- определение контекста Организации;
- разработка структуры документации ИБ;
- разработка типов и видов активов;
- разработка категорий безопасности документации;
- разработка модели ролей культуры ИБ;
- анализ структурного подразделения ИБ;
- рекомендации по разработке корпоративного глоссария культуры ИБ.
2. Разработка политики ИБ в состав услуг входит:
- разработка политики ИБ;
- проведение разъяснений участникам культуры ИБ.
3. Анализ процессов и активов в состав услуг входит:
- разработка основных и вспомогательных процессов;
- декомпозиция процессов на операции;
- определение владельцев процессов и ответственных исполнителей;
- разработка реестра информационных активов;
- разработка карты связанных активов.
4. Разработка базы требований ИБ
5. Анализ оценки рисков в состав услуг входит:
- разработка карты рисков;
- разработка моделей угроз;
- определение моделей нарушителей;
- определение потенциального ущерба;
- разработка системы оценки рисков;
- разработка оценки рисков;
- определение уровня приемлемости ущерба;
- разработка стратегии обработки рисков.
6. Работа с активами в состав услуг входит:
- разработка правил обращения с активами;
- разработка требований по защите активов;
- разработка типологии документов;
- разработка системы маркирования и категорирования.
7. Разработка процедур СУИБ в состав услуг входит:

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе

- разработка процедуры регистрации инцидентов;
- разработка процедуры управления инцидентами;
- создание журнала регистрации инцидентов;
- разработка процедуры корректирующих действий;
- разработка процедуры управления документацией;
- разработка процедуры эффективности СУИБ;
- разработка процедуры непрерывности бизнеса;
- разработка процедуры внутреннего аудита;
- разработка процедуры анализа со стороны руководства.

8. Разработка процедур HR в состав услуг входит:
- разработка процедур уведомления сотрудников о СУИБ;
- разработка процедур проверки знаний правил ИБ (аттестация).

9. Внутренний аудит- разработка процедур проведения внутреннего аудита.

10. Разработка ежегодного графика мероприятий ИБ в состав услуг входит:
- разработка графика мероприятий ИБ;
- разработка графика пересмотра эффективности процедур;
- разработка графика пересмотра целей ИБ;
- разработка графика пересмотра документов;
- разработка графика проведения оценки рисков;
- разработка графика проведения внутреннего аудита;
- разработка графика аттестации сотрудников.

11. Разработка положения о применимости - разработка положения о применимости согласно пунктам международного стандарта ISO/IEC 27001.

12. Разработка карты технической защиты в состав услуг входит:
- разработка политики защиты конечных станций;
- разработка политики защиты сетевой инфраструктуры;
- разработка политики защиты почтового трафика;
- разработка политики управления изменениями;
- разработка политики управления учётными записями;
- разработка политики безопасного хранения данных;
- разработка политики управления инцидентами;
- разработка политики предотвращения утечки информации;
- разработка политики безопасности корпоративных приложений;
- разработка политики управления уязвимостями;
- разработка политики удаленного доступа;
- разработка политики контроля доступа;
- разработка карты физической защиты.

13. Определение соответствующих правовых требований в состав услуг входит:
- определение требований законодательства РК;
- определение требований регуляторов.

8 Требования к исполнителю:
Исполнитель должен предоставить Заказчику все отчеты о результатах проведения аудита, включающий чек-лист несоответствий и рекомендации по их устранению.

9 Место оказания услуг
Адрес оказания услуг: г. Нур-Султан, офис АО «Самрук-Энерго», пр.Кабанбай батыра, 15А, бизнес центр «Q».

10 Сроки оказания услуг
С даты заключения договора в течении 30 рабочих дней.

Приложение

ТС_Аудит по IT.docx

Подписал	Тажин Алмат Болатович
Дата подписания	23.10.2020

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе