ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 514077 , Работы по внедрению системы анализатора сетевых аномалий способом Открытый тендер на понижение

Лот № 1 (111-4 Р, 1816286)

Заказчик: Акционерное общество "Казахстанская компания по управлению электрическими сетями" (Kazakhstan Electricity Grid Operating Company) "KEGOC"
Организатор: Акционерное общество "Казахстанская компания по управлению электрическими сетями" (Kazakhstan Electricity Grid Operating Company) "KEGOC"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	111-4 Р
Наименование и краткая характеристика	Комплексные работы в сфере информационных технологий «под ключ», Комплексные работы в сфере информационных технологий «под ключ», включающая: поставку программного обеспечения, консалтинговые услуги по внедрению информационной системы и поставку оборудования (при необходимости)
Дополнительная характеристика	Работы по внедрению системы анализатора сетевых аномалий
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Нур-Султан, г.Нур-Султан, проспект Тәуелсіздік, 59; 2. г. Нур-Султан, ул. Ушконыр, здание 3/2; 3. г. Актобе, пр. 312-й Стрелковой дивизии, 44; 4. г. Алматы, ул. Шевченко, 162/7; 5. г. Караганда, ул. Камская, 4; 6. г. Усть-Каменогорск, ул. Бажова, 67; 7. г. Шымкент, ул. Б. Момышулы, 27; 8. г. Экибастуз, ул. Ауэзова, 126; 9. г. Рудный, ул. Топоркова, 31; 10. г. Атырау, ул. Махамбета Өтемісұлы, 110а.
Условия поставки	-
Срок поставки	С даты подписания договора в течение 60 календарных дней
Условия оплаты	Предоплата - 30%, Промежуточный платеж - 0%, Окончательный платеж - 70%

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

1. Общие требования
Все предложенные характеристики Системы должны соответствовать или превосходить минимальные технические характеристики, указанные в настоящей технической спецификации.
Система анализатора сетевых аномалий (далее – Система) должна быть реализована в виде программного комплекса, который состоит из программного обеспечения (далее – ПО), размещаемого на серверном оборудовании Заказчика.
Система архитектурно должна строиться на базе двухуровневой архитектуры, которая состоит из:
1) Центрального сервера управления, который должен быть иерархически каскадным, что обеспечивает централизованное управление и видимость для каждого региона с глобальной системой централизованного управления наверху, которая, в свою очередь, обеспечивает глобальную видимость и визуализацию полученных метаданных с сенсоров. Центральный сервер должен обеспечивать механизм обновления ПО и баз сигнатур для промышленного оборудования, которая должна предупреждать основные типы атак на оборудование: отказ в обслуживании (denial of service), заражение вредоносным ПО (malware infection), атака «бокового смещения» (lateral movement), атаки типа command and control (C2 malware), и другие, без необходимости подключения и установки обновлений на каждый сенсор.
2) Сенсоры должны передавать траффик в центр анализа аномалий, располагаемых на уровне доступа к промышленной сети, полученных от промышленного оборудования и других устройств в промышленной сети. Передача трафика от промышленного оборудования должна происходить при помощи зеркалирования трафика от существующего сетевого оборудования на сенсор. Результатом глубокого анализа пакетов должны служить метаданные. Сенсоры должны быть пассивными, то есть не должны влиять на работу промышленной сети.

Центральный сервер управления и сенсоры в количестве 20 (двадцать) штук должны быть выполнены в виде программно-аппаратного комплекса (ПАК) и установлены в соответствии с согласованным с Заказчиком перечнем на объекты Заказчика.
Работы по настройке Системы должны быть выполнены, в соответствии с согласованным с Заказчиком графиком.

2. Технические характеристики и требования к системе
2.1. Требования к функциональным возможностям:
2.1.1. Система должна поддерживать следующие технологические протоколы:
BACNET, CAPWAP, Citect HMI, DHCP, DNP3, EPM, ETHERNET / IP, Foundation Fieldbus, HART-IP, HSRP, HTTP, HTTP-XML,

IEC101, IEC103, IEC104, LLDP, MMS (IEC-61850), Modbus, Modbus Execload, MQTT, NetBIOS Browser, NetBIOS Datagram Service, OPC-DA/UA, POP3, Profinet DCP, Profinet I/O, Profinet Real-Time, PTP, Radius, RTCP, SIP, Skinny, SNMP, SSH, Synchrophasor, TFTP, DMS System, HC800 (Infininet), Melody, Bailey, MasterBus 300, RNRP, Spirit, Symphony Plus, TotalFlow, Alspa Multicast Messages, E-Terra, Altus ALnet, ClearSCADA ViewX, B&R INA2000, AMS (ADS), BSAP, NASNavigator, Caterpillar AHS, SLMP, (CC Link IE Field Basic) CC Link IE – Field, CPHA (Checkpoint High Availability), Discovery Protocol (CDP), UDLD, Cognex Discovery, Comtrol NS Link, Control Technologies, Cygnet SCADA, Dropbox LAN-sync, Modbus Eltec, DeltaV, Ovation, ROC Plus, Telnet- DeltaV, Foxboro LLC, Foxboro RTV, GE Bentley Nevada (BNC3500), GE PAC8000 (AXE), GE SDI (MarkVie), GE SDI Classic (MarkVie), GE SRTP GE-ALM, GE-EGD, GE-EGD-CMP, Modbus GE Enervista, QuickPanel (TRAPI + HTTP), Discovery Protocols, HiDiscovery Telnet – Hirschmann, CIFS (SMB), DCE RPC, DCE RPC - ABB DCS, Service Manager, NTLMSSP (Auth Protocol), Microsoft RDP, SAMR, TDS, Windows Update Delivery Optimzation, Goose (IEC-61850), Sampled Values (IEC-61850), C200 – ftebcip, EpicMo (C300 mgmt), Experion – CeeNTComm, Firewall CF9, HP Switch, Modbus Concept, Modbus Modsoft, Modbus Schneider, Schneider NetManage, Triconex Tristation, Digsi 4, Digsi , P2, PCS7 WinCC – Historian, S7Comm, S7Comm Plus, Siemens FWL Load (Firmware Upload), T3000 Protocols, Modbus ScadaPack, odeq, VNET (VHF), CIP, ENIP, PCCC, DPI (over PCCC), rx3i,9030 Proficy Machine, rx3i,9030 PacsAnalyzer, Bently Nevada 3500 System Configuration, MarkVI ToolBox, ST Siprotec Digsi4 / Digsi5, S7/T3000 Step7, S7 TiaPortal (v13/v14/v15), M221 SoMachine, TwidoSuite, TSX Micro, Premium PL7, SCADAPack 32, Modicon/Quantum, Concept, GP-3000 GP-Pro EX, GP-4000 GP-Pro EX, SP-5000 GP-Pro EX, LT-3000 GP-Pro EX, LT-4000 GP-Pro EX, ST-3000 GP-Pro EX, IPC (PC/AT), SCL.

2.1.2. Система должна поддерживать следующие IP-протоколы:
B&R Profile, B&R Query, BACnet Discovery, BACnet Query, Beckhoff Query, CIP Query, Cisco Profile, Cognex Query, CTI Query, DNP3, ENIP Query, ENIP Scan, Hirschmann Discovery Query, Hirschmann Discovery Scan, Hirschmann Profile, HTTP Query, IoT Query, Mitsubishi Melsoft Query, Mitsubishi Profile, Modbus Information Object, Net Bios, Ping Sweep, Profinet-DCP Query, Profinet-DCP Scan, Rockwell Profile, S7Comm Query, Schneider TSX Query, Schneider Unity Query, Siemens Profile, Siprotec 5 Profile, Siprotec Query, SNMP Network Layout Query, SNMP Query, SNMP Scan, SNMP Siprotec 5, SSH Discovery, TCP Port Discovery, TCP Port Scan, Telnet, VMware ESX Discovery, Windows Profile, WinRM Query, WMI Query, WSD Discovery, WSD Query.

2.1.3. Система должна поддерживать следующих производителей технологических систем:
ABB, Alstrom, AVIVA, Altus, Rockwell, Bristol, B&R, Beckhoff, Buffalo, CC Link IE, Checkpoint, Cisco, Cygnet, Emerson, Eltec, General Electric, Foxboro, Honeywell, Hirschmann, TwinSoft, Schweitzer, Redlion, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa.

2.1.4. Система должна предлагать простоту развертывания без необходимости установки в разрыв и изменения маршрутов сетевого технологического трафика.

2.1.5. Система должна обеспечивать низкую сложность конфигурации / настройки.

2.1.6. Система должна предлагать развертывание в виде виртуального устройства.

2.1.7. Система должна предлагать многоуровневый подход к развертыванию, позволяющий централизованно просматривать все данные на уровне сайта, региона и мира.

2.1.8. Решение должно определять VLAN и автоматически назначать узлы в соответствующие зоны для виртуальной сегментации.

2.1.9. Решение должно назначать идентификаторы VLAN, когда теги VLAN не присутствуют в копии трафика.

2.1.10. Решение должно осуществлять пассивный мониторинг сети в реальном времени.

2.1.11. Решение должно предоставлять топологию/карту всех активов и коммуникаций, а также фильтровать по группам активов и сетевым зонам.

2.1.12. Решение должно идентифицировать коммуникационные потоки (например, IP-адреса и порты источника и получателя, а также протокол) и направление потоков посредством пассивного анализа данных сетевого трафика (например, захват сетевых пакетов, netflow трафика и трафика межсетевого экрана).

2.1.13. Решение должно позволять просмотр тысячи устройств в реальном времени без снижения производительности.

2.1.14. Там, где это применимо, решение должно обеспечивать отображение каналов связи, включая соответствующие коды функций и переменные.

2.1.15. Решение должно включать обнаружение изменений конфигурации контроллера, модификации, запуски/остановки устройства.

2.1.16. Решение должно обеспечивать обнаружение трафика межсетевого экрана и высокую скорость повторной передачи.

2.1.17. Решение должно предоставлять статистику трафика, включая пропускную способность, скорость повторной передачи и общую скорость передачи.

2.1.18. Решение должно обеспечивать отслеживание сессий и статистику.

2.1.19. Решение должно отображать события, происходящие в сети, в хронологическом порядке и с возможностью сравнения различных профилей нормального поведения в разных временных промежутках.

2.1.20. Система должна включать возможность принимать захваченные пакеты и отображать их так, как если бы сеть отслеживалась в реальном времени.

2.1.21. Решение должно давать возможность показать, как карта активов выглядела в прошлом периоде времени, для сравнения изменений в топологии с течением времени.

2.1.22. Решение должно определять сетевые характеристики активов (включая IP-адрес, MAC-адрес, имя хоста, операционную систему, прошивку, поставщика, серийный номер, модули ПЛК, роль устройства) посредством пассивного мониторинга сетевого трафика в реальном времени. (например, копия трафика, данные трафика NetFlow и межсетевого экрана).

2.1.23. Решение должно идентифицировать промышленные активы (OT) (например, устройства ввода-вывода, PLC, RTU, IED) посредством пассивного мониторинга сетевого трафика в реальном времени (например, копия трафика, данных трафика netflow и межсетевого экрана).

2.1.24. Решение должно идентифицировать активы интернета вещей (IOT) (например, камеры, датчики, интеллектуальные устройства, системы управления зданием) посредством пассивного мониторинга сетевого трафика в реальном времени.

2.1.25. Решение должно определять тип и версию операционной системы/прошивки ИТ, IoT и OT посредством пассивного мониторинга сетевого трафика в реальном времени (например, копия трафика, данных трафика netflow и межсетевого экрана).
2.1.26. Решение должно обнаруживать как устройства внутри отслеживаемой сети, так и устройства, которые взаимодействуют с активами, находящиеся за пределами сетей пользователя.
2.1.27. Решение должно обнаруживать сетевые компоненты, которые могут быть обнаружены только пакетами ARP.
2.1.28. Решение должно выявлять уязвимости в активах посредством пассивного анализа данных сетевого трафика (например, копия трафика, данных трафика netflow и межсетевого экрана) в сочетании с анализом угроз.
2.1.29. Решение должно иметь возможность получать данные из внешних источников управления уязвимостями.
2.1.30. Решение должно каталогизировать и классифицировать обнаруженные и существующие уязвимости на основе серьезности и риска, используя такую информацию, как классификация данных и критичность бизнеса, в дополнение к технической информации, такой как влияние, тип уязвимости и векторы атак.
2.1.31. Решение должно обеспечивать автоматическое обнаружение новых хостов, устройств или каналов связи.
2.1.32. Решение должно обеспечивать автоматическое обнаружение новых переменных и значений в известных каналах связи ICS.
2.1.33. Решение должно обеспечивать автоматическое обнаружение изменений поведения в профиле устройств IoT.
2.1.34. Решение должно обеспечивать автоматическое обнаружение изменений поведения в профиле устройств OT.
2.1.35. Решение должно позволять динамически или вручную задавать периоды обучения.
2.1.36. Решение должно обеспечивать аналитику быстрое обновления обучения на основе известных изменений.
2.1.37. Решение должно уметь определять аномалии на основе определенного профиля устройства.
2.1.38. Решение должно иметь возможность настраивать обнаружение аномалий на основе зон.
2.1.39. Решение должно быть дополнено знаниями об активах, чтобы обеспечить точное обнаружение аномалий.
2.1.40. Оповещения об аномалиях должны включать автоматический захват пакетов для просмотра и анализа.
2.1.41. Система должна включать стандартные правила для обнаружения вторжений.
2.1.42. Система должна позволять автоматическое и ручное обновление правил, включая импорт сторонних и пользовательских правил.
2.1.43. Система должна позволять автоматическое и ручное обновление правил YARA, включая импорт сторонних и пользовательских правил.
2.1.44. Система должна иметь сигнатуры для обнаружения угроз для устройств IT, IoT и OT.
2.1.45. Система должна позволять запрашивать любые метаданные, захваченные системой.
2.1.46. Система должна иметь подсистему создания запросов, которая позволяет пользователю легко создавать и выполнять запросы через графический интерфейс по любым метаданным, захваченным системой.
2.1.47. Возможность запроса должна включать функцию автозаполнения и возможность сохранять общие запросы.
2.1.48. Запросы должны позволять создавать виджеты, которые можно использовать в настраиваемых панелях мониторинга и отчетности.
2.1.49. Система должна включать возможность создания настраиваемых предупреждений на основе любого условия или параметра захваченных метаданных.
2.1.50. Система должна проводить автоматическую корреляцию или группировку инцидентов.
2.1.51. Оповещения должны иметь возможность детализации отдельных оповещений, графическое отображение задействованных хостов, информацию о хостах и связанные оповещения.
2.1.52. Оповещения должны включать возможности подтверждения, в том числе возможность подтверждать, что событие связано с изменением инфраструктуры, обновляя базовые параметры сети и активов.
2.1.53. Оповещения должны включать файлы PCAP, записанные для всего события, вызвавшего оповещение для расследования.
2.1.54. Система должна позволять пересылку событий через syslog, snmp trap.
2.1.55. Система должна позволять назначать разные профили безопасности для видимости предупреждений для каждой зоны.
2.1.56. Система должна иметь разные профили безопасности, определяющие разные уровни видимости предупреждений в зависимости от их типа.
2.1.57. Система должна включать SAML в качестве поставщика аутентификации для поддержки единого входа для внешних объектов.
2.1.58. Система должна включать RestFullAPI для интеграции экспорта и приема со стандартными сторонними инструментами и приложениями.
2.1.59. Система должна включать встроенную возможность интеграции стандартных инструментов SIEM, включая McAfee.
2.1.60. Система должна включать встроенную возможность интеграции для автоматической блокировки соединений для стандартных межсетевых экранов нового поколения.
2.1.61. Система должна включать возможность импорта активов в формате файла CSV.
2.1.62. Система должна включать готовую возможность интеграции для систем ticket management, включая ServiceNow.
2.1.63. Система должна включать возможность импорта файлов проекта (автономные ресурсы), SCD / SCL, Yokogawa, Rockwell Harmony (.conf), Yokogawa CENTUM VP (.gz, .zip), Siemens (.cfg), IEC 61850 SCL / SCD (.scd), Triconex (.pt2), Allen-Bradley (.l5x).
2.1.64. Система должна предоставлять настраиваемую панель мониторинга и управления с комплексным обзором показателей, уязвимостей или поставщик может настраивать панель мониторинга и управления в соответствии с требованиями заказчика.
2.1.65. Система должна иметь встроенные готовые отчеты с предопределенным содержанием, которые могут быть созданы пользователем при необходимости и загружены в формате PDF.
2.1.66. Система должна иметь отчеты, основанные на настраиваемых запросах, которые можно загрузить в формате PDF или запланировать циклическое создание.
2.1.67. Решение должно обеспечивать простую настройку отчетности без необходимости владения языком программирования. Он также должно давать возможность создавать повторяющиеся выполнения настраиваемых запросов для генерации предупреждений.

2.1.68. Система должна иметь готовые шаблоны отчетов о критических мерах безопасности.
2.1.69. Система должна иметь настраиваемый поиск через графический интерфейс без необходимости предварительного знания SQL или аналогичного языка.
2.1.70. Компонент отчетности должен формировать отчеты в форматах PDF и CSV.
2.1.71. Система должна иметь возможность делать резервные копии.
2.1.72. Система должна шифровать все данные при передаче.
2.1.73. Система должна соответствовать рекомендациям, предложенным NIST.
2.1.74. Система должна обеспечивать механизмы аварийного восстановления и резервного копирования данных в случае потери или повреждения данных.
2.1.75. Система должна обеспечивать удаленный доступ к критически важным системам и конфиденциальным данным только по защищенным каналам (например, HTTPS).
2.1.76. Система должна использовать проприетарную оболочку или операционную систему с отраслевыми стандартами безопасности и криптографическими механизмами для обеспечения более высокого уровня безопасности.
2.1.77. Система должна быть надежно настроена и усилена за счет использования отраслевых стандартов (например, удаление ненужных служб; изменение учетных данных по умолчанию; сложность пароля; отключение любых радиоинтерфейсов, если они есть) и соблюдения корпоративных политик безопасности.
2.1.78. Система должна иметь возможность отправлять журналы безопасности и функциональные журналы в SIEM на SOC.
2.1.79. Система должна разрешать удаленное управление только по защищенным каналам (например, HTTPS).
2.1.80. Система должна позволять привилегированным пользователям управлять контролем доступа пользователей.
2.1.81. Система должна выполнять безопасное автоматическое обновление плагинов/данных уязвимостей, сигнатур и платформы уязвимостей. Система должна регулярно выполнять безопасные исправления и обновления программного обеспечения.
2.1.82. Система должна обеспечивать синхронизацию данных и согласование временных меток через всемирное координированное время (UTC).
2.1.83. Система должна инициировать коммуникационный поток от сенсора к центральной консоли.
2.1.84. Поставщик платформы должно предоставлять обновления для операционной системы и приложения в одном образе обновления.
2.1.85. Система должна обеспечивать аутентификацию через стандарты LDAP и LDAPS.
2.1.86. Поставщик Системы должен предоставить полное решение, содержащее все необходимые компоненты (операционная система и необходимые приложения, такие как веб-сервер и база данных), без необходимости установки и обслуживания дополнительного программного обеспечения.
2.1.87. Система должна обеспечивать механизм обновления с центральной консоли управления без необходимости подключения и установки обновлений на каждый датчик.
2.1.88. Система должна поддерживать централизованную систему управления, которая может быть иерархически каскадной, что обеспечивает централизованное управление и видимость для каждого региона с глобальной системой централизованного управления наверху, которая, в свою очередь, обеспечивает глобальную видимость.
2.1.89. Резервное копирование и восстановление платформы должно быть доступно с помощью интерфейса командной строки или веб-консоли (GUI).
2.1.90. Сенсоры должны поддерживать следующие функциональные возможности: сегментация сети, построения site-to-site VPN туннелей, IPS, IDS. Должны поддерживаться следующие механизмы обнаружения угроз: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения. Контроль приложений, база данных управления приложениями должна содержать не менее 8000 известных приложений.
2.1.91. Архитектура решения должна поддерживать масштабирование от 100 устройств до более 10 000 устройств.

2.2. Аппаратные и рабочие требования к сенсору:
• 8x1 Гбит LAN портов;
• 1x1 Гбит опциональный оптический либо медный порт;
• 1x1 WAN порт;
• USB 3.0 порт;
• USB-C консольный порт;
• 12V – коннектор питания;
• поддержка SD карты расширения памяти;
• встроенный 3/4G/LTE модем;
• поддержка 2 SIM-карт (Nano и Micro) с возможностью автоматического переключения между ними в случае потери связи;
• пропускная способность в режиме IPS и контроля приложений - минимум 950 Мбит/с;
• датчик должен работать в диапазоне температур от -40 до +75 градусов;
• датчик должен иметь степень защиты оболочки IP30.

3. Требования к технической поддержке
3.1. Комплектация Системы, включая встроенное ПО, необходимые лицензии и подписки, должна включать предусмотренные производителем техническую поддержку на срок не менее 36 месяцев со дня активации лицензий.
3.2. Техническая поддержка должна обеспечивать:
• доступ к обновлениям версий встроенного ПО;
• возможность прямого обращения в службу технической поддержки производителя методом обращений через специализированный портал.

4. Прочие характеристики
4.1. Потенциальный поставщик в технической спецификации тендерной заявки должен указать:
4.1.1. Полное наименование всех дополнительных модулей в составе предлагаемой к поставке Системы;
4.1.2. Полное наименование специализированного программного обеспечения, предлагаемой к поставке Системы;
4.1.3. Потенциальный поставщик в заявке на участие в тендере должен предоставить авторизационное письмо от производителя Системы или уполномоченного лица на территории РК о том, что имеет право перепродавать/распространять лицензионное ПО производителя на территории РК.
4.2. Поставщик одновременно с поставкой должен предоставить лицензии о праве использования Системы конечным Заказчиком на территории РК.
4.3. Поставщик должен предоставить документы по описанию конфигурации и руководства по эксплуатации Системы. Разработать и согласовать программу и методику испытаний Системы, сценарии функционального и технологического тестирования Системы, регламент администрирования.
4.4. Провести обучение ключевых и конечных пользователей Системы с подготовкой программы и материалов для проведения обучения.

5. Прочие требования:
5.1. Поставщик должен выполнить поставку и внедрение Системы в соответствии с настоящей технической спецификацией в полном объеме.
5.2. Поставщик обязан при поставке Системы осуществить установку и настройку ПО.
5.3. В целях безопасности сети допуск для оказания сопутствующих услуг будет выдаваться сертифицированным специалистам по поставляемой Системе.
5.4. Система должна быть интегрирована с существующим оборудованием Заказчика и модулем управления Системы.
5.5. Поставщик после подписания договора должен предоставить список специалистов, которые будут выполнять работы, а также менеджера, непосредственно занимающегося данным проектом.
5.6. Поставщик должен разработать план внедрения, с обеспечением наименьшего времени простоя технологической сети во время установки и настройки ПО.
5.7. Поставщик должен представлять отчеты об оказанных сопутствующих услугах (план установки и настройки Системы), предварительно структуру отчета согласовывать с Заказчиком.
5.8. Предлагаемая Система должна инсталлироваться и внедряться Поставщиком.
5.9. Поставщик обучает администрированию и работе с системой не менее 5-ти работников Заказчика.

6. Проверка и испытание:
6.1. Поставщик при поставке Системы, должен выполнить работы по установке и настройке Системы «под ключ» в срок не более 60 рабочих дней с даты предоставления необходимой материально-технической базы со стороны Заказчика. После завершения указанных работ Заказчик совместно с Поставщиком проводит проверку Системы на функциональное соответствие настоящей технической спецификации с подписанием акта выполненных работ.
6.2. Поставщик должен выполнить тестирование Системы с предоставлением протоколов функционального и технологического тестирования, реестра результатов тестирования и протокола тестирования информационной безопасности.

7. Гарантийные обязательства
7.1. Гарантийный срок на поставляемую Систему не менее 36 месяцев с даты активации лицензии.

3. Технические стандарты

№ п/п	Зарегистрирован в РК	Обозначение	Номер документа	Категория	Наименование	Область применения	Разработчик	Страницы	МКС	Статус	Приказ	Дата введения с	Дата по
1	Да	СТ РК ISO/IEC 27001-2015	384044	Национальный стандарт Республики Казахстан	Информационная технология методы и средства обеспечения безопасности системы менеджмента информационной безопасностью	Настоящий стандарт устанавливает требования к разработке, внедрению, поддержанию в рабочем состоянии и непрерывному совершенствованию системы менеджмента	Нет ()	68	Наборы знаков и кодирование информации	Действует	Приказом Председателя Комитета технического регулирования и метрологии Министерства по инвестициям и развитию	01.01.2017	

					требования	информационной безопасностью организации в контексте существующих бизнес рисков организации.					Республики Казахстан от 24 ноября 2015 г. № 236-од		

Подписал Сүйінбай Жандос Талғатұлы
Дата подписания 22.12.2020