ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 446041
способом Открытый тендер на понижение

Лот № (56-1 У, 1566187) Услуги по предоставлению лицензий на право использования программного обеспечения

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

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	56-1 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения по предотвращению утечки конфиденциальных данных
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 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ
Услуги по предоставлению лицензий на право использования программного обеспечения

Код ЕНС ТРУ 582950.000.000001

1. Предмет закупки
Услуги по предоставлению лицензий на право использования программного обеспечения по предотвращению утечки конфиденциальных данных.

2. Объем и характеристики закупаемых услуг
2.1. Программное обеспечение для обеспечения контроля и предотвращения утечки конфиденциальных данных предназначен для обнаружения и блокирования передачи конфиденциальной информации. Конфиденциальность данных идентифицируется по различным, заранее определенным признакам и параметрам. Программное обеспечение для обеспечения контроля и предотвращения утечки конфиденциальных данных состоит из двух программных компонентов и лицензии к ним.

Таблица 1. Перечень товаров
№ Наименование услуг Технические характеристики услуг, содержащий в обязательном порядке указанную в плане закупок дополнительную характеристику Ед. из-ния Кол-во
1 2 3 4 5
Услуги по предоставлению лицензий на право использования программного обеспечения Услуг по предоставлению лицензий на право использования программного обеспечения по предотвращению утечки конфиденциальных данных.
Лицензии на компоненты системы предотвращения утечки конфиденциальных данных и контроля автоматизированных рабочих мест – 380 шт.
При оказании услуг должны входить лицензии на среду виртуализации – 1 шт., которая должна включать серверные ОС – 2 шт., а также лицензию на базу данных – 1 шт.
услуга 1

3. Требования к оказанию услуг по предоставлению лицензий на право использования программного обеспечения по предотвращению утечки конфиденциальных данных, в том числе требования к программному обеспечению (далее – Система).
3.1. Требования к архитектуре Системы:
3.1.1. Система должна относиться к классу Enterprise DLP систем и иметь как функционал защиты конечных точек от утечек

конфиденциальной информации с помощью устанавливаемого на конечные точки агента (Endpoint DLP), так и функционал контроля утечки конфиденциальной информации по сетевым каналам (Network DLP).
3.1.2. Система по защите от утечки конфиденциальной информации должна быть агентским решением, устанавливаемым на конечные точки;
3.1.3. Система должна поддерживать функционал дополнительного контроля утечки конфиденциальной информации по сетевым каналам;
3.1.4. Управление модулями Системы должна осуществляться посредством веб браузера;
3.1.5. Система должна иметь возможность централизованного управления агентами.
3.2. Требования к функционалу Системы:
3.2.1. Система должна поддерживать защиту конечных точек, работающих под управлением:
– Операционные системы Microsoft: Windows (Desktop/Server) официально поддерживаемые, на момент внедрения системы, производителем операционной системы;
– Операционные системы Linux: Linux (Desktop/Server) в том числе самые популярные версии: Debian, Red Hat, SUSE, Ubuntu и тд;
– Операционные системы MacOS X.
3.2.2. Система должна поддерживать защиту конечных точек, работающих под управлением операционных систем в среде Virtual Desktop Infrastructure.
3.2.3. Система должна поддерживать обнаружение конфиденциальной информации на всех конечных точках, работающих под управлением ОС Windows (Desktop/Server), Linux (Desktop/Server), Mac OSX, в БД, SharePoint, file shares (Windows, Samba, CIFS, NFS).
3.2.4. Система должна обеспечивать обнаружение конфиденциальной информации в файлах графических изображений с помощью встроенного модуля OCR. Этот функционал не должен требовать приобретения отдельной лицензии.
3.2.5. Система должна поддерживать интеграцию с Microsoft Active Directory.
3.2.6. Система должна поддерживать защиту конфиденциальных данных от утечек в облачных хранилищах данных и облачных сервисах.
3.2.7. Система должна поддерживать защиту конфиденциальной информации от утечек при работе с облачными сервисами и облачными хранилищами данных.
3.2.8. Система должна поддерживать следующие методы классификации данных (Data Classification):
– автоматический, базирующийся на контексте (например, на основе информации о местонахождении файла с конфиденциальной информацией);
– автоматический, базирующийся на контенте (содержимом файла/e-mail);
– базирующийся на файловых операциях (тег классификации определяется маршрутом перемещения файла или e-mail);
– определяемый приложением (тег классификации определяется приложением, которое создает/модифицирует файл);
– определяемый принадлежностью файла/e-mail пользователю/группе пользователей;
– пользовательский (пользователь вручную может классифицировать файл или e-mail в процессе его создания или после). Этот функционал должен быть реализован встроенной интеграцией в агент на конечной точке стандартного функционала классификации данных. (лицензия на этот функционал на этом этапе не должна включаться, но предлагаемое программное обеспечение должно поддерживать этот функционал за счет масштабирования путем покупки соответствующей лицензии в будущем).
3.2.9. Система должна поддерживать интеграцию с системами SIEM/Log Management:
– Система должна поддерживать экспорт событий нарушений ИБ и сигналов тревоги в SIEM/Log Management-системы, используя протокол и формат Syslog;
– Система должна поддерживать экспорт событий нарушений ИБ и сигналов тревоги в SIEM-системы в «родном» для них формате (например, ArcSight CEF, QRADAR LEEF, Splunk CIM).
3.2.10. Механизм обнаружения конфиденциальной информации должен поддерживать следующие методы идентификации информации:
– по строкам, ключевым словам, регулярным выражениям, словарям;
– по цифровым отпечаткам;
– по контекстной классификации;
– по точному и полному совпадению.
3.2.11. Система должна поддерживать тегирование файлов / электронных почтовых отправлений.
3.2.12. Тегирование должно поддерживаться на основных типах файлов:
– Adobe Acrobat – pdf;
– Ansi Text – txt;
– ASF - asf;
– CSV (Comma-separated values) - csv;
– HTML – htm, html;
– MHT-архивы (HTML-архивы, сохраненные Internet Explorer) – mht;
– Microsoft Access 2007 – accdb;
– Microsoft Excel – xls, xlsb, xlsm, xlsx, xml, xps;
– Microsoft Word for Windows – doc; docm; docx;
– Формат архивов – zip; zipx; rar;
– Файлы изображений - jpeg, jpg, bmp, gif, tif, tiff;
– Формат временного файла – tmp;
– C++ Source Code File – cpp;

– Microsoft Dynamic Link Library – dll;
– Word Document Template – dot, dotx, dotm;
– Artboard Drawing – flv;
– C/C++/Objective-C Header File – h;
– Log File – log;
– NES Sound Format File – nsf;
– Microsoft PowerPoint Template – pot, potm, potx;
– Microsoft PowerPoint Add-in – ppa, ppam;
– Microsoft PowerPoint Slide Show – pps, ppsm;
– Microsoft PowerPoint Presentation – ppt; pptm; ppts; pptx;
– Mac OS X Printable File – prn;
– Microsoft Outlook Personal Information Store File – pst;
– Microsoft Publisher Document – pub;
– Microsoft Rich Text Format File – rtf;
– Microsoft Symbolic Link File – slk;
– Microsoft Visio – vsd, vsdx, vss, vssx, vstx, vsx;
– Steinberg VST Audio Plugin – vst;
– VTX Chiptune File – vtx;
3.2.13. Результат классификации должен быть оформлен в виде тега;
3.2.14. Тег должен сохраняться вне зависимости от манипуляций с объектами тегирования;
3.2.15. Присвоенный тег должен наследоваться;
3.2.16. Должна поддерживаться множественность тегов, отражающая результат различных методов классификации, применяемых к одному и тому же объекту тегирования;
3.2.17. Теги должны быть видимы даже в случае архивации файлов (например, в ZIP/RAR-формат);
3.3. Требования к модулю контроля утечек на конечных точках:
3.3.1. Защита конечных точек от утечки конфиденциальных данных, обнаружение конфиденциальных данных на конечных точках, классификация данных – должны быть функционалом одного агента, устанавливаемого на конечную точку.
3.3.2. Агент Системы должен поддерживать возможность активации защиты от целенаправленных атак, путем активации дополнительных лицензий не входящих в поставку.
3.3.3. Система должна понимать и контролировать взаимосвязи между родительскими и дочерними процессами программ на конечных точках (лицензия на этот функционал на этом этапе не должна включаться, но предлагаемое программное обеспечение должно поддерживать этот функционал за счет масштабирования путем покупки соответствующей лицензии в будущем).
3.3.4. Система должна уметь анализировать параметры командной строки с целью пресечения запуска команд, нарушающих политики информационной безопасности (лицензия на этот функционал на этом этапе не должна включаться, но предлагаемое программное обеспечение должно поддерживать этот функционал за счет масштабирования путем покупки соответствующей лицензии в будущем).
3.3.5. Система должна уметь контролировать вызовы различных DLL-библиотек приложениями на конечных точках и блокировать эти вызовы в случае возникновения рисков нарушения политик безопасности.
3.3.6. Система должна уметь контролировать вывод на печать конфиденциальной информации.
3.3.7. Система должна уметь контролировать обмен конфиденциальной информацией между различными приложениями на конечных точках, реализуемый командами Cut, Copy, Paste, Insert, PrintScreen.
3.3.8. Система должна уметь контролировать перемещения конфиденциальной информации, блокировать операции копирования конфиденциальной информации и/или производить шифрование переносимой конфиденциальной информации на следующих видах внешних накопителей информации:
– съемные жесткие диски;
– USB диски и Flash накопители;
– карты памяти;
– CD/DVD и флоппи-диски.
3.3.9. Функционал шифрования данных на съемных устройствах не должен требовать приобретения отдельной лицензии.
3.3.10. Устанавливаемый на конечных точках агент должен иметь (при необходимости) возможность работы в “невидимом” для пользователя режиме.
3.3.11. Удаление устанавливаемого на конечных точках агента без соответствующей авторизации должно быть исключено даже в случае наличия администраторских привилегий на конечной точке.
3.3.12. Система должна контролировать использование конфиденциальной информации любыми приложениями, работающими на конечных точках:
– Почтовые клиенты: Microsoft Outlook, IBM Lotus;
– Web-браузеры: Firefox, Google Chrome, Internet Explorer;
– Офисные приложения: Microsoft Office Word, Microsoft Office Excel, Microsoft Office Powerpoint, Acrobat Reader, Instant Messengers и т. д.
3.3.13. Система должна обеспечивать контроль операций с файлами Copy, Move, Save As, Open, Close, Read, Write, и Edit на конечных точках для предотвращения утечек конфиденциальной информации.
3.3.14. Система должна контролировать попытки выгрузки и загрузки конфиденциальной информации с конечных точек в ЛВС, облачные хранилища, Интернет-ресурсы.
3.3.15. Система должна поддерживать возможность защиты конечных точек от целенаправленных атак (лицензия на этот

функционал на этом этапе не должна включаться, но предлагаемое программное обеспечение должно поддерживать этот функционал за счет масштабирования путем покупки соответствующей лицензии):
– обеспечивать анализ аномального поведения приложений и пользователей на конечных точках;
– иметь возможность интеграции со сторонними решениями (например, Palo Alto, Virus Total, FireEye) для получения информации о различных видах вредоносных программ;
– контролировать и блокировать распространение вредоносных программ;
– блокировать попытки доступа вредоносных программ к конфиденциальной информации;
– наличие пред настроенной панели киберугроз.
3.3.16. Система должна обеспечивать контроль работы приложений на базе черных и белых списков.
3.4. Требования к модулю контроля утечек по сетевым каналам:
3.4.1. Система должна поддерживать инспекцию почтового трафика путем получения трафика от агента пересылки сообщений
3.4.2. Система должна уметь инспектировать следующие характеристики почтового трафика:
– заголовки почтовых сообщений;
– тему письма;
– тело письма;
– вложение.
3.4.3. Система должна поддерживать следующие контроли:
– возможность перенаправления исходящих писем на систему шифрования писем сторонних производителей, согласно настроенных политик;
– блокировку сообщений;
– карантин.
3.4.4. Система должна поддерживать мониторинг сетевого (TCP) трафика.
3.4.5. Система должна поддерживать интеграцию с ICAP-совместимыми прокси серверами, включая режимы работы, как forward прокси, так и reverse прокси.
3.4.6. Система должна поддерживать как мониторинг, так и блокировку информации, при работе с веб трафиком.
3.4.7. Система должна поддерживать работу со следующими типами данных:
– Структурированные данные, включая те, что хранятся в базах данных (Oracle DB, Microsoft SQL Server, MySQL, PostgreSQL, DB2, Sybase, Informix) и табличные форматы, такие как csv.
– Неструктурированные данные – письма, презентации, CAD файлы, веб страницы

4. Требования к оказанию услуг по настройке Системы:
4.1. Поставщик должен осуществить настройку компонентов Системы по месту эксплуатации.
4.2. Для оценки ресурсов, необходимых для работы систем – должен быть предоставлен план работ по внедрению, расчет времени, необходимого на внедрение и запуск в эксплуатацию компонентов Системы.
4.3. Инсталляция компонентов системы предотвращения утечки конфиденциальных данных и контроля автоматизированных рабочих мест - при необходимости, должно быть произведено создание виртуальных серверов на базе имеющегося оборудования у Заказчика, установка программного обеспечения систем, контроль и проведение установки агентов на конечные устройства.
4.4. Определение активов для обеспечения информационной безопасности, которые будут контролироваться системами:
4.4.1. Определение совместно с Заказчиком внутренних документов для служебного пользования: политик, порядков, приказов и т.д.;
4.4.2. Определение совместно с Заказчиком периодически поступающих и создаваемых документов делопроизводства: письма, договоры и т.д.
4.5. Пуско-наладочные работы:
4.5.1. Настройка правил компонентов системы предотвращения утечки конфиденциальных данных и контроля автоматизированных рабочих мест на основании определенного перечня активов;
4.5.2. Мониторинг работы компонентов системы предотвращения утечки конфиденциальных данных и контроля автоматизированных рабочих мест, оценка эффективности работы настроенных правил и последующая оптимизация после запуска DLP-системы.
4.6. Определение активов для обеспечения информационной безопасности, которые будут контролироваться системами:
4.6.1. Определение совместно с Заказчиком внутренних документов для служебного пользования: политик, порядков, приказов и т.д.;
4.6.2. Определение совместно с Заказчиком периодически поступающих и создаваемых документов делопроизводства: письма, договоры и т.д.
4.7. Поставщик должен предоставить Заказчику возможность контроля и надзора за ходом выполнения настроек.
4.8. Поставщик должен немедленно известить Заказчика и до получения от него указаний, приостановить настройки, при обнаружении: - возможных неблагоприятных для Заказчика последствий выполнения его указаний о способе выполнения настроек; - иных, не зависящих от Поставщика обстоятельств, угрожающих годности или качеству результатов внедрения Системы, либо создающих невозможность завершения их в срок.
4.9. Поставщик осуществит обучение трех сотрудников Заказчика по администрированию и настройки Системы;
4.10. Поставщик должен провести тестирование Системы на отслеживание дефектов и иных недочётов и предоставить исполнение в виде отчета;
4.11. Поставщик должен провести функциональное тестирование Системы для проверки исполнений всех требований технической спецификации и предоставить исполнение в виде отчета;

5. Требования к потенциальному поставщику
5.1. Потенциальный поставщик в составе заявке на участие в закупках должен предоставить полную спецификацию с указанием всех требуемых лицензий, количества и всех составных частей, требуемых данной технической спецификацией;
5.2. Потенциальный поставщик в составе заявке на участие в закупках должен предоставить подтверждающее письмо, что он является авторизованным партнером на право поставки лицензионного программного обеспечения, предлагаемой Системы.

6. Срок поддержки лицензий обновления – 12 месяцев.

7. Место оказания услуг
Услуги должны быть оказаны Заказчику по адресу:
г. Нур-Султан, офис АО «Самрук-Энерго», пр.Кабанбай батыра, 15А, бизнес центр «Q»

8. Сроки оказания услуг
С даты заключения договора в течении 30 календарных дней.

Подписал	Тажин Алмат Болатович
Дата подписания	04.06.2020