**Приложение №1**

**к Технической спецификации**

**Описание и требуемые функциональные, технические, качественные и**

**эксплуатационные характеристики**

**В техническую поддержку входят услуги на продление лицензий и техническую поддержку (далее техническая поддержка) McAfee/Forcepoint Sidewinder в том числе:**

1. McAfee ePolicy Orchestrator
2. Forcepoint Sidewinder
3. McAfee Network Security Platform
4. McAfee VirusScan Enterprise
5. McAfee Host Intrusion Prevention
6. McAfee Web Gateway
7. McAfeeVirtual ATD add on for Web Security, Gateway Edition Software

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Срок продления лицензий** | **Срок оказания технической  поддержки McAfee/Forcepoint Sidewinder** | **Наименование товара** | **Количество** |
| **1** | **2** | **3** | **4** | **5** |
| 1 | C 01.01.2021 по  31.12.2021 года включительно | С даты подписания Договора по 31.12.2021 года, распространяет свое действие на использование Заказчиком лицензии McAfee с 01.01.2021 года | Sidewinder S1104 Appliance Extended Warranty - Advanced RMA (12 months), 1 Units, Sidewinder Appliance, 12 Months, Renewal | 1 |
| 2 | C 01.01.2021 по  31.12.2021 года включительно | Network Security Premium Support + Maintenance, 1 Units, Tech Support, 12 Months, Renewal | 1 |
| 3 | C 01.01.2021 по  31.12.2021 года включительно | MFE Network Sec Starter Mngr 1Yr GL [IMTYCM-AD- AA] | 1 |
| 4 | C 01.01.2021 по  31.12.2021 года включительно | MFE Cloud Workload Sec Adv 1YrBZ[P+] [CWAYFM-AB-AA] | 20 |
| 5 | C 01.01.2021 по  31.12.2021 года включительно | MFE vATD for WSG Add On 1:1 BZ [V02ECE-AA-EA] | 400 |
| 6 | C 01.01.2021 по  31.12.2021 года включительно | MFE Web Security 1Yr BZ [WSGYCM-AA-EA] | 400 |
| 7 | C 01.01.2021 по  31.12.2021 года включительно | MFE Endpoint Protection - Adv 1YrBZ[P+] [EPAYFM-AA-EA] | 400 |

Перечень оказываемых Исполнителем услуг:

**В техническую поддержку системы информационной безопасности построенной на программно-аппаратном комплексе McAfee/Forcepoint Sidewinder входят следующие услуги, но не ограничиваются ими:**

1. поддержка работоспособности системы информационной безопасности ТОО «АлматыЭнергоСбыт»;
2. оказание технической поддержки при возникновении проблем при администрировании специалистами Заказчика программно-аппаратного комплекса системы информационной безопасности ТОО «АлматыЭнергоСбыт»;
3. оказание помощи в установке модулей и подсистем программно-аппаратного комплекса McAfee/ Forcepoint Sidewinder;
4. обновление по запросу Заказчика программно-аппаратного комплекса McAfee/ Forcepoint Sidewinder до актуальных версий, выпускаемых Производителем, в течение 7 календарных дней с даты выхода обновлений;
5. определение характера проблем, возникающих у Заказчика при эксплуатации Системы и предоставление Заказчику письменного решения для их локализации;
6. оказание помощи в изменении настроенных политик безопасности Системы по запросу Заказчика;
7. настройка автоматического резервного копирования данных в пределах обслуживания оборудования McAfee/ Forcepoint Sidewinder;
8. документирование всех вносимых изменений со стороны Исполнителя в программно-аппаратный комплекс, с передачей документации Заказчику;
9. осуществление помощь по запросу Заказчика по обновлению версий программно-аппаратного комплекса McAfee/Forcepoint Sidewinder до последней актуальной версии продукта выпущенной Производителем и последующая проверка функционирования Системы после ее обновления осуществляется при участии специалистов Заказчика. Обновление Системы должно быть произведено с сохранением всех произведенных Заказчиком настроек на программно-аппаратном комплексе McAfee/ Forcepoint Sidewinder;
10. обновление и/или изменения в Системе производится Исполнителем с предварительным согласованием сроков и процедур обновления с Заказчиком;
11. консультирование сотрудников Заказчика по всем возникающим вопросам в работе программно-аппаратного комплекса McAfee;
12. проверка системных параметров и настроек Системы, при необходимости производится полная переустановка программного обеспечения;
13. консультирование при диагностике неисправностей, выработке решений по их устранению;
14. предоставление доступа к порталу [Service Portal McAfee](https://mysupport.mcafee.com/Eservice/Default.aspx);
15. доступ к McAfee Global Solutions Lab;
16. доступ к Deployment Assistance Program – DAP;
17. доступ к личному кабинету Forcepoint осуществляется через портал: <https://support.forcepoint.com/MyAccount>
18. информирование Заказчика по электронной почте о выходе обновлений версий программно-аппаратного комплекса McAfee/ Forcepoint Sidewinder;

Сопровождение и администрирование центральной консоли управления системы информационной безопасностью McAfee ePolicy Orchestrator

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Создание и заполнение групп в дереве систем, поддержка актуального состояния дерева систем | Обслуживание и структурированная организация дерева систем путем создания иерархических, объеденных по логическим признакам коллекцию систем. Добавление новых систем к существующей группе, поддержка дерева систем в актуальном состояние, своевременное удаление выбывших систем. |
| 2 | Настройка и применение политик для управления продуктами и системами из единого расположения - центральной консоли управления системы информационной безопасности | Управление политиками McAfee ePolicy Orchestrator посредством применения политик к управляемым системам путем наследования или назначения на основе пользователя, на основе системы. |
| 3 | Развертывание продуктов и обновлений | Инфраструктура репозиториев McAfee ePolicy Orchestrator позволяет развертывать продукт и обновлять пакеты в управляемых системах из централизованного местоположения. |
| 4 | Создание, редактирование и удаление панелей мониторинга | Использование панелей мониторинга позволяет осуществлять постоянное наблюдений за средой. |
| 5 | Подготовка и настройка запросов к базе данных и отчетов о состоянии системы | Используя инструменты Построитель отчетов и Построитель запросов возможно создавать, редактировать и выполнять запросы и отчеты, результатами которых являются настраиваемые данные, диаграммы и таблицы. Данные для таких отчетов и запросов могут быть получены из зарегистрированной базы данных в системе McAfee ePolicy Orchestrator. |
| 6 | Экспорт/ Импорт объектов из/в McAfee ePolicy Orchestrator. | Репликация поведения с одного сервера McAfee ePolicy Orchestrator на другой путем экспорта элемента, описывающего поведение и импорт его на другом сервере. |
| 7 | Настройка исходных и резервных сайтов | Для поддержания программного обеспечения информационной безопасности в актуальном состоянии необходимо проводить настройку исходных и резервных сайтов для получения обновлений и сигнатур безопасности. |

Сопровождение и администрирование Межсетевого экрана McAfee Firewall Enterprise

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Настройка правил контроля доступа | Создание, редактирование и удаление правил межсетевого экрана, отвечающих за сопоставления правил доступа с сетевыми соединениями и обработки соединений согласно настроенным правилам. Сетевые соединения, которые не соответствуют правилам доступа, должны блокироваться. |
| 2 | Настройка реестра сетевых объектов | Создание, редактирование и удаление компонентов, используемых в качестве основных элементов правил контроля доступа. |
| 3 | Настройка списка и групп приложений | Для классификации сетевых соединений и обработки |
| 4 | Настройка антивирусного сканирования | Осуществление проверки на вирусы на сетевых интерфейсах межсетевого экрана McAfee Firewall Enterprise, являющихся границами сетевых сегментов. |
| 5 | Настройка VPN | Обеспечение защищенной передачи данных через незащищенные сети используя процесс шифрования и дешифрования с поддержкой протокола IPsec. |

Сопровождение и администрирование системы защиты от вторжений McAfee Network Security Platform

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Настройка и управление политиками IPS | Используя политики IPS производится настройка защиты от определенных уязвимостей и DoS-атак, типов автоматического реагирования, необходимого для блокировки дальнейшего воздействия. |
| 2 | Настройка оповещений об обнаруженных уязвимостях | Создание и редактирование сигнальных уведомлений на консоль управления системы защиты от вторжений в случае обнаружения угроз уязвимости. |
| 3 | Настройка оповещений об обнаруженных DoS-атак | Создание и редактирование сигнальных уведомлений на консоль управления системы защиты от вторжений в случая обнаружения DoS атаки. |
| 4 | Настройка расширенного обнаружения бот-сетей | Использование функций обнаружения бот-сетей. |

Сопровождение пользовательских антивирусов McAfee VirusScan Enterprise

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Предотвращение проникновения угроз в клиентские системы. Защита точек доступа к системе. | Защита доступа предотвращает нежелательные изменения на компьютере путем ограничения доступа к указанным портам, файлам, общим ресурсам, разделам и значениям реестра операционной системы. |
| 2 | Настройка правил блокировки портов | Правила блокировки портов предотвращают доступ пользователей к портам входящего и исходящего трафика, а также доступ других компьютеров к данному компьютеру. |
| 3 | Настройка правил блокировки реестров | Правила блокировки реестров не позволяют пользователям и неавторизованным программам изменять, открывать или удалять определенные разделы и значения реестров. |
| 4 | Настройка политик защиты от атак с переполнением буфера | Осуществление защиты от переполнения буфера предотвращает выполнение произвольного кода на компьютерах Общества при переполнении буфера. |
| 5 | Настройка обновлений определений обнаружений | Для определения угроз и принятия по отношению к ним необходимых действий программное обеспечение VirusScan Enterprise использует механизм сканирования и информацию в файлах определения обнаружений (DAT). Новые угрозы появляются постоянно. В ответ на это McAfee ежедневно выпускает новые файлы DAT, содержащие результаты постоянного исследования угроз. Задача обновления позволяет получать самые последние файлы DAT с внешнего сайта обновлений McAfee и устанавливать их на локальный сервер. |

Сопровождение системы обнаружения и предотвращения вторжений на компьютеры сети McAfee Host Intrusion Prevention

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Настройка политик межсетевого экрана | Применяя политики межсетевого экрана McAfee Host Intrusion Prevention возможно осуществлять включение и выключение правил для предотвращения вторжений. Обеспечение безопасности путем фильтрации входящего и исходящего трафика сетевых систем с установленными операционными системами. |
| 2 | Настройка политик IPS | Политики IPS включают и выключают защиту от вторжений, задают уровни ответа на разные типы событий и обеспечивают защиту путем применения исключений, сигнатур и правил защиты приложений. |

Сопровождение системы защита от веб угроз McAfee Web Gateway

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Настройка, редактирование белого списка для правила фильтрации URL – адресов | Создание, редактирование списка веб-сайтов, доступ к которым разрешен. |
| 2 | Настройка, редактирование черного списка правил фильтрации URL – адресов | Создание, редактирование списка веб-сайтов, отмеченных в определенной категории, которая не предназначена для использования. |
| 3 | Настройка правил фильтрации URL адресов на основе белых и черных списков | Создание, редактирование правил фильтрации URL-адресов, которые позволяют идентифицировать определенные в черных списках типы веб-сайтов, содержащих недопустимые материалы, и позволяют разрешать или блокировать доступ к этим веб-сайтам на основании предварительно заданных категорий URL-адресов. |
| 4 | Настройка списков блокировки доступа клиентских хостов | Создание, редактирование списков клиентских хостов не имеющий доступ к ресурсам Интернет. |
| 5 | Настройка списков фильтрации по содержимому контента | С целью блокирования веб-сайтов с содержимым, не предназначенным для просмотра, фильтрации сайтов по их содержимому, создание и редактирование списка содержащего реестр запрещенного контента. |
| 6 | Настройка правил фильтрации по содержимому контента | Создание правил в системе, не позволяющих получить доступ к определённым сайтам или услугам сети Интернет на основе списков фильтрации по содержимому контента. |
| 8 | Формирование отчетов посещения web-сайтов | Формирование отчетности отображающей статистические данные об использовании web-траффика. |
| 9 | Конфигурирование системы | По мере необходимости проводится конфигурирование системных настроек аппаратно-программного комплекса системы защиты от веб угроз через пользовательский интерфейс или интерпретатор командной строки. |
| 10 | Управление конфиденциальной  информацией с помощью правил  защиты | Правила защиты контролируют поток данных, определяя действие, которое выполняется при попытке перенести или передать конфиденциальные данные. |

Сопровождение системы защиты электронной почты и антиспама

| № | Наименование услуги | Описание |
| --- | --- | --- |
| 1 | Настройка фильтрации протокола SMTP | Конфигурирование основных настроек для протокола SMTP, настройка параметров прозрачности и обработки сообщений. |
| 2 | Настройка безопасности входящих сообщений | Создание, редактирование списков  разрешенных и запрещённых соединений, списков  разрешенных и запрещённых отправителей, конфигурирование настроек Anti-Relay,  аутентификации получателей. |
| 3 | Настройка безопасности исходящих сообщений | Создание, редактирование списка маршрутизации почты, добавление MX записи, конфигурирование настроек Anti-Relay. |
| 4 | Настройка политик почты для протокола SMTP и POP3 | Создание политик для выявления и блокирования спама, вирусов, вредоносных программ, фишинга, атак с целью сбора существующих адресов. Конфигурирование политик антивируса, антиспама, выполнения политик. |

Резервное копирование и восстановление системы информационной безопасности

|  |  |  |
| --- | --- | --- |
| № | Наименование услуги | Описание |
| 1 | Обслуживание базы данных McAfee ePolicy Orchestrator | Для обеспечения оптимальной производительности и защиты данных необходимо выполнять периодическое обслуживание баз данных: резервное копирование и восстановление баз данных McAfee ePolicy Orchestrator. Еженедельное регулярное копирование базы данных логов системы информационной безопасности. |
| 2 | Резервное копирование и восстановление конфигурации межсетевого экрана Forcepoint Sidewinder | Ежеквартальное регулярное резервное копирование конфигурации межсетевого экрана. По мере необходимости восстановление конфигураций межсетевого экрана Forcepoint Sidewinder. |
| 3 | Обслуживание базы данных системы предотвращения вторжений McAfee Network Security Manager | Мониторинг сетевой безопасности является непрерывным процессом, требующим архивирования и поддержания в актуальном состоянии базы данных событий, генерируемых McAfee Network Security Sensor. |
| 4 | Восстановление резервной копии базы данных логов при наличии базы резервной копии СУИБ | По мере возникновения необходимости осуществлять восстановление резервной копии базы данных логов СИБ из имеющейся у Заказчика резервной копии. |

Администрирование системы информационной безопасности

|  |  |  |
| --- | --- | --- |
| № | Наименование услуги | Описание |
| 1 | Управление сертификатами | По мере необходимости проводить подготовку, импорт и назначение сертификатов безопасности используемых для идентификации и сверки сетевых хостов во время сетевых коммуникаций. |
| 2 | Установка дополнительных клиентских мест – агентов политик безопасности | Развертывание агентов на клиентские места в случае возникновения необходимости (при установке, переустановке операционных систем). |
| 3 | Телефонные консультации Заказчика | По мере возникновения необходимости телефонные проводятся консультации пользователей СИБ в оперативном режиме. |

Доступность услуг и обработка поступающих обращений

1) Запросы и заявки Заказчика осуществляются по телефону, электронной почте и через web – интерфейс - с 8:30 до 19:00 времени Астаны в течение рабочей недели (рабочей неделей считается понедельник пятница, исключение составляют праздничные дни согласно законодательству РК);

* В случае невозможности решения вопроса по телефону, инженер Исполнителя должен быть направ­лен непосредственно на место возникновения проблемы.
* Время реагирования на месте расположения Системы при неисправностях (сбоях) не должно превышать четырех часов.
* В случаях, если Система может эксплуатироваться Заказчиком с ограниченными функциями, и при этом Исполнитель предложено временное или обходное решение, то инцидент должен быть устранен в течение 7 рабочих дней с момента принятия данного обращения.
* В последствие, временное решение проблемы заменяется на полноценное.
* В прочих случаях, незначительно влияющих на функционирование Системы, Исполнитель обязуется устранить их в течение 10 рабочих дней.
* В каждом случае превышения «Времени устранения» по обращению Заказчика, Исполнитель подписывает акт закрытия заявки (обращения) у Заказчика после выполнения восстановительных работ и/или устранения сбоев/ошибок в работе Системы.