**ПРИГЛАШЕНИЕ № 86**

**к участию в конкурсе с неограниченным участием**

Дата: «17» ноября 2022 г.

**ЗАО «Альфа телеком»** (далее - Компания) приглашает правомочных поставщиков представить свои конкурсные заявки на закупку **услуг** **по внедрению** **DLP системы** (далее Приглашение).

Описание предмета закупки, характер, перечень, количество, место и сроки поставки, требования, предъявляемые к поставщикам и иные требования установлены **в Требованиях к закупке (приложение 1 к Приглашению**).

1. Для участия в конкурсе необходимо:

|  |  |  |
| --- | --- | --- |
| **Подать конкурсную заявку**  в электронном виде согласно Требованиям к закупке (приложение 1)  с установлением пароля доступа | **По эл. адресу:**  **tender@megacom.kg** | **Дата окончания приема конкурсных заявок:**  **25.11.2022г. 13:59 часов (GMT+6)** |
| **Направить пароль** для доступа к конкурсной заявке | **По электронному адресу:**  **tender@megacom.kg** | **Дата окончания приема паролей к конкурсным заявкам:**  **25.11.2022г. с 14:00 до 15:59 часов (GMT+6)** |
| **Вскрытие конкурсных заявок состоится:** | по адресу: г. Бишкек, ул. Суюмбаева, 123; | ***ДАТА и Время вскрытия конкурсных заявок: 25.11.2022г. в 16:00*** |

***Вложенный файл (конкурсная заявка) не должен превышать 10мб, в случае превышение рекомендуется разделить и отправить несколькими сообщениями (письмами) или воспользоваться облачными файлообменниками***

1. При наличии вопросов по настоящему Приглашению поставщик может обратиться в Компанию по электронному адресу: **tender@megacom.kg** за получением разъяснений, но не позднее 3 рабочих дней до истечения окончательного срока представления конкурсных заявок. Разъяснения направляются обратившемуся поставщику по электронной почте, с которой был получен запрос, не позднее трех календарных дней с момента получения запроса.
2. При необходимости, Компания вправе внести изменения в настоящее Приглашение путем издания дополнений в любое время до истечения окончательного срока представления конкурсных заявок, но в любом случае не позднее 3 (трех) рабочих дней.
3. Компания может перенести окончательную дату подачи конкурсных заявок на более поздний срок, если вносятся поправки в настоящее Приглашение, о чем Компания информирует путем размещения соответствующей информации на официальном сайте Компании и информационном ресурсе, где было размещено объявление о проведении настоящего конкурса.
4. **Порядок подачи конкурсной заявки.** Поставщику, желающему участвовать в конкурсе необходимо согласно Требованиям к закупке (приложение 1 к Приглашению) заполнить конкурсную заявку (приложение 2 к Приглашению), приложить требуемые копии документов, установить к ним пароль доступа и отправить в электронном виде на электронную почту, указанную в п. 1 Приглашения, не позднее установленного срока. При этом, Поставщик обязуется сообщить/направить Компании пароль доступа не позднее установленного срока и вышеуказанным способом.

Каждый участник конкурса может подать только одну конкурсную заявку.

1. Компания может установить фиксированную сумму гарантийного обеспечения конкурсной заявки (далее – ГОКЗ). Срок действия ГОКЗ должен совпадать со сроком действия конкурсной заявки. Данное требование устанавливается при необходимости.

ГОКЗ вносится в размере и форме, предусмотренных в конкурсной документации.

ГОКЗ возвращается не позднее трех рабочих дней в случаях:

1) истечения срока действия конкурсной заявки, указанного в конкурсной документации;

2) заключения договора и предоставления ГОИД, если предоставление такого гарантийного обеспечения предусмотрено в конкурсной документации;

3) отзыва конкурсной заявки до истечения окончательного срока представления конкурсных заявок;

4) прекращения процедур закупок без заключения договора.

5. Гарантийное обеспечение конкурсной заявки закупающей организацией удерживается в случаях:

1) отказа подписать договор на условиях, предусмотренных в конкурсной заявке победителя, за исключением случаев, если такой отказ связан с введением режима чрезвычайной ситуации или чрезвычайного положения, при условии опубликования объявления о закупке до введения таких режимов;

2) отказа предоставить гарантийное обеспечение исполнения договора;

3) отзыва конкурсной заявки после ее вскрытия и до истечения срока ее действия;

4) изменения условий конкурсной заявки после вскрытия конвертов с конкурсными заявками.

1. **Конкурсные заявки, поданные поставщиками позднее указанного срока и/или заявки, к которым не сообщен пароль до установленного срока, не принимаются и не рассматриваются.**

**Подавая свою конкурсную заявку, поставщик тем самым выражает свое согласие на все условия, указанные в проекте (-ах) договора (-ов) (Приложение 3 к Приглашению).**

**Не допускается внесение изменений в конкурсные заявки после истечения срока их подачи.**

1. Поставщик, подавший конкурсную заявку, может присутствовать на вскрытии конкурсных заявок. На вскрытии конкурсных заявок оглашается цена конкурсной заявки, а также список документов, приложенных к конкурсной заявке, и вносится в протокол вскрытия.
2. Во время оценки конкурсных заявок Компания вправе обратиться к поставщику за разъяснениями по поводу его конкурсной заявки. Запрос о разъяснениях и ответ на него должны подаваться в письменном виде по электронной почте.
3. Оценка конкурсных заявок осуществляется в соответствии с процедурами и критериями, предусмотренными в Требованиях к закупке (приложение 1 к Приглашению). Компания вправе запросить у поставщика исправление арифметических ошибок, допущенных в конкурсной заявке.

В случае если по итогам проведенной оценки поставщиками предоставлены конкурсные заявки с одинаковыми ценами и условиями, отвечающие требованиям конкурсной документации, то Компания направляет поставщикам, представившим одинаковые цены запрос по электронной почте о возможности снижения цены (предоставления скидки), выигравшей конкурсной заявкой считается заявка поставщика, предоставившего наименьшую цену (наибольшую скидку). В случае если после снижения цены (предоставления скидки) поставщики представили одинаковые предложения (цена, скидка), то победитель определяется посредством случайной выборки.

1. Компания отклоняет конкурсную заявку в случаях, если:

- участник, представивший конкурсную заявку, не соответствует квалификационным требованиям, установленным в Требованиях к закупке (приложение 1 к Приглашению);

- конкурсная заявка по существу не отвечает требованиям, установленным в Требованиях к закупке (приложение 1 к Приглашению);

- технические параметры, предложенные в конкурсной заявке, не соответствуют технической спецификации, установленной в Требованиях к закупке (приложение 1 к Приглашению);

- поставщик представил более одной конкурсной заявки;

- поставщик не предоставил гарантийное обеспечение конкурсной заявки;

- цена конкурсной заявки превышает планируемую сумму закупки;

- в случае выявления конфликта интересов согласно п. 6.5 Правил организации и осуществления закупок в ЗАО «Альфа Телеком».

1. Конкурс признается Компанией несостоявшимся в случаях, когда были отклонены все предложения поставщиков, не поступило ни одного предложения или минимальная цена по конкурсу превышает планируемую сумму закупки.
2. Компания может отменить конкурс в любое время до заключения договора, если отпала необходимость в дальнейшем приобретении предмета закупки.
3. Компания в течение двух рабочих дней с момента подведения итогов по конкурсу направляет поставщикам по электронной почте уведомления: победителю о том, что его заявка признана победившей, остальным участникам, что их заявки не признаны победившими.
4. Поставщик, определенный победителем конкурса, должен подтвердить уведомление о признании его победителем в течение трех рабочих дней путем направления ответного письма по электронной почте.
5. В случае нарушения победителем сроков: подтверждения заключения договора, подписания договора/возврата экземпляра договора Компании или внесения гарантийного обеспечения исполнения договора, Компания вправе заключить договор с поставщиком вторым в рейтинге.
6. Поставщик, участвующий в конкурсе, имеет право подать жалобу Компании относительно требований конкурсной документации не позднее двух рабочих дней до даты окончательного срока подачи конкурсных заявок или проведенной оценки по конкурсу не позднее двух рабочих дней после подведения итогов по конкурсу. Жалоба поставщика рассматривается Компанией в срок до 3-х рабочих дней. В случае несогласия поставщика с решением Компании по жалобе, поставщик вправе обратиться в судебные органы.

Приложение:

1. Требования к закупке
2. Форма конкурсной заявки
3. Проект договора

**Руководитель отдела по закупкам М. Кенжебаев**

*Исп.: Н. Шаршенов*

*Тел:0312 905 244*

**Приложение 1 к Приглашению**

**Требования к закупке**

|  |  |  |
| --- | --- | --- |
| **1.Общие требования** | | |
| 1.1 | Язык конкурсной заявки | Русский **(в случае если документ будет составлен на** иностранном языке, необходимо предоставить дополнительно перевод на русском языке) |
| 1.2 | Условия, место и срок поставки | Электронным способом на эл. почту **не позднее десяти рабочих дней с даты заключения Договора**: [InfSecurity@megacom.kg](mailto:InfSecurity@megacom.kg) направляется уведомление о предоставлении права пользования программным обеспечением, лицензиями и технической поддержкой |
| 1.3 | Срок предоставления услуг | С даты подписания Акта приема-передачи выполненных услуг, сроком на 12 месяцев |
| 1.4 | Условия оплаты и срок выплаты | 100% от цены договора выплачиваются в течение 10 банковских дней со дня получения счета-фактуры, выставленного на основании и датой подписания сторонами Акта, подтверждающего право пользования программным обеспечением и лицензиями.  **Оплата осуществляется:**   * Поставщику-нерезиденту: Доллар США или другая иностранная валюта. * Поставщику-резиденту в сомах КР:   Оплата осуществляется путем перечисления денежных средств на расчетный счет Поставщика.  \*При оплате нерезидентам КР за Лицензии на ТП/услуги при отсутствии межгосударственных соглашений об избежание двойного налогообложения будет удержан налог на доход иностранной организации по ставке 10%. |
| 1.5 | Цена конкурсной заявки | *В цену, указанную участниками конкурса, должны быть включены все налоги, сборы и другие платежи, взимаемые в соответствии с законодательством Кыргызской Республики, а также накладные расходы* |
| 1.6 | Валюта конкурсной заявки | **Для резидентов КР:** Сом КР\* (\*Примечание: Если резидентом КР будет подана конкурсная заявка в другой валюте, то договор будет заключен в национальной валюте по курсу Национального банка КР на день вскрытия).  **Для нерезидентов КР:** Доллар США или другая иностранная валюта.  \*Оценка будет производиться в национальной валюте - сом по курсу Национального банка КР на день вскрытия конкурсных заявок. |
| 1.7 | **Для Юридических лиц**, копии документов, определяющих организационно-правовую форму юридического лица, место регистрации и основной вид деятельности:   * Свидетельство о гос. регистрации/перерегистрации, * Устав * Приказа/решение/протокол об избрании/назначении исполнительного органа юр.лица (1-го лица)   **Для индивидуальных предпринимателей**: Свидетельство о регистрации в качестве индивидуального предпринимателя или действующий патент (при этом вид деятельности должен совпадать с предметом закупки и охватывать минимум период до полной поставки товара и передачи по акту) | Приложить копии (в случае если, данные документы составлены на иностранном языке, необходимо предоставить дополнительно перевод на русском языке). |
| 1.8 | Доверенность на лицо, подписавшее конкурсную заявку и представляющее интересы участника в торгах (если она подписывается не исполнительным органом – руководителем компании) | Приложить скан копию доверенности. |
| 1.9 | Авторский надзор, Технический надзор, или контроль за ходом выполнения работ/услуг, поставки товаров | После получения сообщения по эл. почте представителю ЗАО «Альфа Телеком» опредоставленииправа пользования программным обеспечением, лицензиями и технической поддержкой, Заказчик осуществляет проверку полученных прав на соответствие Спецификации на интернет-портале производителя ПО. При соответствии прав пользования Спецификации,Заказчик подписывает Акт приема-передачи в течение 2-х рабочих дней |
| 1.10 | Срок действия конкурсной заявки, в календарных днях | 60 (шестьдесят) календарных дней с даты вскрытия конкурсных заявок |
| 1.12 | Размер и форма гарантийного обеспечения исполнения договора (ГОИД) | Поставщик, которому будет присуждено право заключения договора, по итогам конкурса должен внести гарантийное обеспечение исполнения договора (ГОИД), в виде денежных средств, в размере:  **3** **%** от общей суммы Договора путем перечисления денежных средств на банковский счет Компании в течение 5 банковских дней с даты заключения Договора.  **Гарантийное обеспечение исполнения договора или его остаток  после удержания начисленных неустоек и/или сохранения  части суммы ГОИД на период технической поддержки\* возвращается Исполнителю не позднее десяти рабочих дней с даты  подписания Акта приема передачи  оказанных услуг. \*На период действия срока технической поддержки, закупающая организация сохраняет  у себя сумму гарантийного обеспечения исполнения договора в размере 10% от внесенной Исполнителем суммы гарантийного обеспечения исполнения договора после заключения договора**  *Порядок возврата ГОИД определяется в договоре.* |
| 1.13 | Критерии оценки | 1. \* Победившей может быть признана Конкурсная заявка, отвечающая по существу требованиям **конкурсной документации, квалификационным требованиям, техническим параметрам и имеющая наименьшую оцененную стоимость\*.**   \* при определении оцененной стоимости, от общей стоимости конкурсной заявки вычитается НДС (-12%), если участник-резидент КР является плательщиком НДС, соответственно, оценка заявок будет проводиться без учета НДС-12%. |
| **1.14** | **Другие необходимые документы, которые участники конкурса должны заполнить и предоставить** | **Заполнить: 1. Таблицу соответствия техническим требованиям (Приложение 2.1 к Приглашению);**  **2.Форму конкурсной заявки (Приложение № 2 к Приглашению)** |
| 1.15 | Условия договора | См. проект Договора (Приложение № 3) |
| **1.16** | **Выделяемая сумма** | **10 735 000 сом** |
| **2. Квалификационные требования** | | |
| 2.1 | Опыт аналогичных по характеру и степени сложности предоставлении услуг, в денежном выражении | Наличие опыта по характеру аналогичных поставок (услуг) за последние 2 года в сумме не менее 6 млн. (шесть миллионов) сом или эквивалент в долларах США. Подтвердить информацию о выполненных поставках (опыте) необходимо актами приема-передачи или счетами-фактурами. |
| 2.2 | Авторизация: | Приложить действующие авторизационное письмо от Правообладателя/Производителя ПО, действующее на территории КР со сроком авторизации не менее чем срок предоставления услуг.  В случае, если предоставляется авторизационное письмо, выданное не Правообладателем/Производителем ПО, а их дистрибьютором, в целях установления его полномочий необходимо также предоставить авторизационное письмо, выданное данному дистрибьютору Правообладателем/Производителем ПО. |
| **2.3** | **Другие документы** | **Предоставить полный пакет документов на продукт, подтверждающий соответствие техническим требованиям** |
| *\* В случае участия в конкурсе простого товарищества, каждый его участник должен отвечать установленным квалификационным требованиям.* | | |

|  |
| --- |
| **3. Существенные требования/ Технические спецификации** |

**Технические требования  
к системе контроля и предотвращения утечки конфиденциальной информации**

1. **Требования к поставке лицензионных программных средств**
   1. Дистрибутив программного обеспечения должен поставляться с документацией в электронном или печатном виде на русском языке. Документация должна включать в себя правила установки и использования лицензионного программного обеспечения.
   2. Исполнитель должен предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие права на обновление и поддержку (гарантийное сопровождение) программного обеспечения в течение 12 (двенадцати) месяцев.
   3. Лицензии системы должны позволять осуществлять одновременный контроль не менее 400 пользователей.
   4. Подсистемы контентного анализа и принятия решений должны лицензироваться за единицы (одна лицензия на каждую подсистему).
   5. Модули подсистемы контроля должны иметь лицензирование по конечным пользователям, то есть одна лицензия требуется для одной подконтрольной (защищаемой Системой) доменной или локальной учетной записи.
   6. Лицензии модулей подсистемы контроля должны быть конкурентными. Это значит, что одну лицензию можно использовать для контроля разных пользователей (учетных записей) только в разные периоды времени.
   7. Программное обеспечение должно условно состоять из следующих модулей или подсистем:
      1. Подсистема контроля, состоящая из:
   * модуль контроля электронной почты
   * модуль контроля сервисов обмена мгновенными сообщениями
   * модуль контроля FTP-соединений
   * модуль контроля HTTP-трафика (POST- и GET-запросы)
   * модуль контроля печати
   * модуль контроля и управления доступом съёмных устройств
   * модуль контроля событий на мониторах и действий сотрудников
   * модуль контроля разговоров сотрудников (аудиоконтроль)
   * модуль контроля активности пользователей и приложений
   * модуль контроля облачных хранилищ данных
     1. Подсистема контентного анализа
     2. Подсистема принятия решений
2. **Технические требования к Системе**
   1. **Требования к Системе в целом**
      1. Программное обеспечение для защиты информации (Далее – Система) должно обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей. Система должна поддерживать работу на уровне рабочих станций (Endpoint), на уровне сети (получение теневой копии трафика от сетевого оборудования либо прокси-сервера) и на уровне интеграций со сторонними системами (пр. технологий - SMTP, ICAP, API). Система должна предоставлять возможность работы в одном или нескольких перечисленных режимах одновременно.
      2. Система должна быть построена на базе клиент-серверной архитектуры, где сервер выполняет роли администрирования, обработки, хранения и анализа данных, а клиент выполняет роль пользовательского интерфейса или агента.
      3. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Windows:
   * Windows 7 x32/x64;
   * Windows 8, 8.1 x32/х64;
   * Windows 10 x32/х64;
   * Windows 11 х64;
   * Windows Server 2008 R2;
   * Windows Server 2012, 2012 R2;
   * Windows Server 2016;
   * Windows Server 2019.
     1. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Linux:
   * Ubuntu 16.04 x32/x64, 18.04 x64, 20.04 x64, 21.04 x64.
   * CentOS 7.4 x64, 8 x64;
   * Red Hat Enterprise Linux (RHEL) 7 x64;
   * AltLinux 9 x32/x64;
     1. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства MacOS:
   * Mojave 10.14;
   * Catalina 10.15
   * Big Sur 11.0.1;
   * Monterey 12.1.
     1. Система должна иметь потенциал развития и поддержки новых версий популярных версий операционных систем.
     2. В связи с существенной разницей архитектур операционных систем Windows, Linux, MacOS допускается разница между функциями Агента, реализованными для ОС Windows, Linux и MacOS, а также между разными ядрами или версиями ОС Linux.
     3. Все серверные функции Системы должны выполняться в рамках единого решения, СУБД одной версии для архивирования данных и поддерживать установку на операционных системах семейства Windows Server/Linux Server.
     4. Система должна поддерживать работу в замкнутом контуре, то есть в локальной сети Заказчика без выхода в сеть Интернет. Исключением служат отдельные опциональные функции в явном виде требующие интернет-соединения).
     5. Все сетевые соединения, протоколы связи и направления соединений должны быть указаны в технической документации на Систему.
     6. Система должна обеспечивать защиту данных, передаваемых агентскими или клиентскими компонентами по линиям связи.
     7. Система должна не оказывать негативного влияния либо ухудшать основные функциональные характеристики Сети заказчика (надежность, быстродействие, возможность изменения конфигурации, удобство использования);
     8. Система должна обладать характеристиками масштабирования и отказоустойчивости;
     9. Система должна обеспечить интеграцию в существующую у Заказчика вычислительную сеть без изменения топологии сети;
     10. Система должна предполагать возможность установки отдельного модуля по каждому или группе контролируемых каналов передачи данных;
     11. Система должна предполагать возможность выборочной активации модулей контроля для вышеперечисленных каналов передачи данных.
     12. Система должна иметь удобный и понятный пользовательский интерфейс, где все сообщения и документация должны быть на русском языке;
     13. Система не должна оказывать негативного влияния на нормальное функционирование серверов и рабочих станций Заказчика;
     14. Система должна обеспечивать разграничение прав доступа к перехваченной информации, политикам безопасности и настройкам системы;
     15. Система должна обеспечивать контроль веб-трафика на уровне рабочих станций, на уровне интеграций с прокси-серверами по протоколу ICAP и на уровне передачи теневой копии трафика (SPAN) с сетевых шлюзов;
     16. Система должна обеспечивать контроль почтового трафика как на уровне рабочих станций, так и на уровне интеграции с корпоративным почтовым сервером;
     17. Система должна обладать возможностью оптимизации нагрузки на ресурсы территориально разделенных сетей с «узким» каналом передачи данных благодаря предварительному сжатию информации или настройке расписания и скорости ее передачи;
     18. Система должна обеспечивать индексирование документов, перехваченных модулями контроля, для ускорения поиска и обработки событий;
     19. Система должна интегрироваться с Active Directory.
     20. Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах ОС Windows.
     21. Система должна иметь веб-интерфейс при работе с результирующими отчетами Системы, при этом разграничение доступа должно быть централизованным и индивидуальным в веб-интерфейсе.
     22. Для информационного обмена между компонентами системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet).
     23. Система должна обеспечивать блокировку HTTP(S)-трафика на рабочих станциях согласно настраиваемым атрибутивно-зависимым правилам. Тематическая категория блокируемого HTTP(S) ресурса также должна являться атрибутом.
     24. Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах ОС Windows для всех указанных в п. 2.1.3 операционных систем.
     25. Агент Системы, осуществляющий контроль на уровне рабочих станций c ОС Windows, должен быть подписан цифровой подписью.
     26. Подсистема контентного анализа должна предоставлять возможности:
   * проведения ретроспективного анализа архива информации;
   * генерации отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности;
   * просмотра активности пользователей в режиме реального времени.
     1. Подсистема принятия решений должна предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту – нарушает или не нарушает он существующие правила.
     2. Модуль контроля электронной почты должен обеспечивать контроль сообщений электронной почты (протоколы SMTP/ESMTP/SMTPS, POP3/POP3S, IMAP, MAPI), а также иметь подключаемую функцию автоматической остановки отправки сообщения в случае возникновения инцидента, зарегистрированного данным модулем на конечных станциях или посредством интеграции с почтовым сервером.
     3. Модуль контроля сервисов обмена мгновенными сообщениями должен обеспечивать контроль сообщений и файлов, переданных при помощи популярных интернет-мессенджеров. В частности, обеспечивать контроль сеансов текстовой связи, файлов, переданных посредством Skype, контроль чатов, звонков и файлов коммуникационных клиентов Microsoft Lync, Viber, Telegram и Zoom Chat, Whatsapp и др..
     4. Модуль контроля FTP-соединений должен обеспечивать контроль входящего и исходящего FTP-трафика. В случае контроля на уровне рабочих станций также необходима поддержка FTP через SSL (FTPS).
     5. Модуль контроля HTTP-трафика должен обеспечивать контроль POST-запросов при использовании пользователями интернет-сервисов, а также иметь подключаемую функцию автоматической остановки трафика в случае возникновения инцидента, зарегистрированного данным модулем.
     6. Модуль контроля печати должен обеспечивать контроль документов, отправленных на печать при помощи сетевых или локальных принтеров.
     7. Модуль контроля и управления доступом съемных устройств должен обеспечивать контроль файлов, записываемых на USB-устройства, CD/DVD и др. типы съемных устройств.
     8. Модуль контроля событий на мониторах и действий сотрудников должен обеспечивать контроль изображений с экранов пользователей, предоставлять возможность осуществления видеозаписи действий, создания снимков и записи видео посредством веб-камеры, а также предоставлять возможность просмотра содержимого мониторов и действий пользователей за рабочей станцией в режиме реального времени. Модуль должен осуществлять контроль данных, вводимых с клавиатуры, логирование нажатий клавиш в любых приложениях (в том числе нажатия системных клавиш и их сочетаний). В целях обеспечения конфиденциальности, модуль, при наличии технической возможности, должен выделять ввод пароля и давать возможность исключить пароли из аудита.
     9. Модуль контроля разговоров сотрудников должен обеспечивать аудиозапись разговоров с помощью подключенного к рабочей станции микрофона. В целях обеспечения конфиденциальности третьей стороны важно, чтобы модуль позволял выбирать различные настройки своей работы для случаев, когда сотрудник находится в офисе и за его пределами.
     10. Модуль контроля активности пользователей и приложений должен обеспечивать мониторинг активности пользователей и запускаемых ими процессов с учетом длительности в течение рабочего дня.
     11. Модуль контроля облачных хранилищ данных должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов (Google Drive, OneDrive, Office 365, Dropbox, Evernote, Яндекс Диск, cloud.mail.ru и др.), а также позволять контролировать файлы, передаваемые в программах удаленного доступа (TeamViewer, VNC, Radmin, LiteManager).
     12. В Системе должны быть реализованы функции, обеспечивающие управление настройками конфигурации Системы и осуществляющие автоматизированный контроль штатного функционирования Системы. Под управлением понимается комплекс действий, позволяющих сотрудникам Заказчика изменять заданные настройки Системы самостоятельно, без привлечения сторонних специалистов. Под автоматизированным контролем штатного функционирования подразумевается мониторинг штатной работы всех компонентов Системы и автоматическое уведомление администратора в случае нештатных ситуаций.
   1. **Требования к способам и средствам связи для информационного обмена**
      1. Система должна функционировать в составе информационно-вычислительной сети Заказчика.
      2. Модули контроля на уровне рабочей станции должны иметь возможность использования HTTPS для передачи данных на сервер Системы для защиты соединения и/или использовать альтернативные алгоритмы шифрования передаваемых данных.
      3. Система должна корректно работать в сетях с Active Directory.
      4. Система должна поддерживать работу в виртуальной инфраструктуре.
      5. Для информационного обмена между компонентами Системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet).
      6. Для информационного обмена между Системой и корпоративной почтовой системой должен использоваться протокол SMTP.
      7. Система должна предоставлять возможность однозначного определения данных сотрудника компании, отправившего информацию, благодаря интеграции с Active Directory:
   * учетной записи пользователя,
   * информации об использованной рабочей станции (имени, IP- и MAC-адреса).
   1. **Требования по диагностированию Системы**
      1. Система должна обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности.
      2. Каждый модуль Системы должен иметь штатный и расширенный режим записи в журналы. В случае программных сбоев должен быть предусмотрен отладочный режим принудительной записи в системные журналы. Отладочный режим включается автоматически без участия пользователя при наступлении программного сбоя.
      3. В случае многопользовательской работы модуль должен автоматически создавать раздельные журналы для каждого пользователя.
   2. **Перспективы развития и модернизации Системы** 
      1. Система должна допускать наращивание производительности за счет улучшения характеристик технических средств.
      2. Система должна обеспечивать возможность модернизации путем замены технического и/или программного обеспечения.
      3. Исполнитель может привлекаться для консультаций Заказчика для согласования минимально достаточного или рекомендуемого оборудования при планировании внедрения Системы.
   3. **Требования к функциям администрирования**
      1. Интерфейс администратора должен предоставлять возможность контроля работоспособности Системы.
      2. Интерфейс администратора должен предоставлять возможность отображения статистики работы Агентов, серверных подсистем, службы блокировки почты, СУБД, операционной системы с возможностью резервного копирования статистических данных.
      3. Интерфейс администратора должен обеспечивать возможность управления службами подсистем.
      4. Интерфейс администратора должен предоставлять возможность управления базами данных модулей контроля информации.
      5. Интерфейс администратора должен предоставлять возможность мониторинга дискового пространства на серверах Системы.
      6. Интерфейс администратора должен предоставлять возможность автоматического оповещения о важных событиях (сбои в работе, нехватка свободного места, превышение количества лицензий и другие).
      7. Интерфейс администратора должен обеспечивать возможность синхронизации с одним или более доменом Active Directory.
      8. Интерфейс администратора должен обеспечивать возможность работы с пользователями рабочих групп.
      9. Интерфейс администратора должен предоставлять возможность разграничения прав доступа сотрудников службы безопасности к функционалу консолей подсистем и к данным по тем или иным пользователям, группам пользователей, и источникам данных. Под данными подразумеваются зафиксированные подсистемой принятия решений инциденты, а также доступное к просмотру в подсистеме контентного анализа содержимое документов и почтовых сообщений, попавших в карантин.
      10. Интерфейс администратора должен обеспечивать возможность управления настройками функций сбора статистики и предоставления отчетов, а также обеспечивать возможность настройки просмотра отчетов посредством веб-интерфейса.
      11. Интерфейс администратора должен предоставлять возможность автоматического переноса «старых» баз данных, индексов, хранилищ на новое место хранения (с целью разгрузки быстрых дисков), а также осуществление автоматического архивирования баз данных, индексов, хранилищ с последующей возможностью их восстановления.
   4. **Требования к хранению данных**
      1. Для эффективной работы с большими массивами данных Система, когда это технически возможно, должна хранить оригиналы теневых копий файлов в специальном файловом хранилище, адаптированном и оптимизированном для работы с Системой.
      2. Система должна иметь опцию хранения текстовой и атрибутивной информации в специализированных табличных пространствах и индексатор для выполнения полнотекстового поиска в системе. Система должна позволять выполнять поиск событий напрямую из СУБД без ожидания построения индекса в целях минимизации времени расследования инцидента.
      3. Система должна быть совместима с Microsoft SQL Server 2008 SP2, PostgreSQL 13, Oracle 16 и выше для хранения информации в структурированной табличной форме и дальнейшей ее обработки в сторонних системах анализа.
      4. Система должна архивировать все перехваченные объекты, а не только те, по которым зафиксированы инциденты.
   5. **Требования к надежности**
      1. Должен быть предусмотрен типовой регламент действий по восстановлению работоспособности в случае отказов Системы. Процедуры восстановления работоспособности Системы должны быть описаны и задокументированы в соответствующей эксплуатационной документации на Систему.
      2. Система должна быть реализована таким образом и/или определен комплекс мер и мероприятий, обеспечивающих восстановление ее работоспособности и данных при сбоях силами штатного обслуживающего персонала.
      3. В случае возникновения сбоя технического или программного обеспечения Системы должна быть обеспечена возможность восстановления ее данных и настроек.
3. **Требования к функциям (задачам), выполняемым Системой**
   1. **Требования к подсистеме контентного анализа**
      1. Подсистема контентного анализа должна быть ориентирована на работу с данными, получаемыми от модулей подсистемы контроля.
      2. Подсистема должна предоставлять возможность создания политик блокировки (помещения в карантин) трафика электронной почты, передаваемого по протоколу SMTP, а также исходящей почты, передаваемой посредством клиента Outlook по протоколам IMAP и MAPI, до принятия вердикта ответственным лицом.
      3. Подсистема должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных или запротоколированных объектов, обозначенных в разделе 4:
   * поиск, по ключевым словам, и фразам в базах перехваченных документов;
   * выборка перехваченных данных по дате, доменному имени пользователя, адресам и хостам электронной почты, псевдонимам в Мессенджерах, именам компьютеров, принтеров и др. атрибутам;
   * поиск по образцу текста, схожему по смыслу или содержанию с искомым. Данный тип поиска не должен подразумевать никаких манипуляций с настройками поискового механизма и подключения дополнительных словарей, кроме задания процента релевантности (схожести) документов;
   * поиск по набору слов, позволяющий находить документы, содержащие определенное количество либо процент таких слов. Набор слов может быть введен вручную, вставлен из буфера обмена либо загружен из внешнего текстового файла. При формировании каждого отдельного слова из словаря не должны использоваться логические операторы.
   * поиск с использованием отраслевых словарей с группировкой по тематикам
     1. Анализ текстового содержимого должен производиться с учетом морфологических особенностей русского языка. При этом словоформы должны образовываться без использования логических операторов и специальных символов.
     2. Подсистема должна предоставлять возможности для просмотра детальной информации по каждому перехваченному объекту, в том числе возможность просмотра записи действий на экранах пользователей во встроенном видеоплеере.
     3. Подсистема должна предоставлять возможность просмотра контентного маршрута перехваченного документа.
     4. Подсистема должна предоставлять возможности экспорта выборки перехваченных данных (полного списка или набора файлов с оглавлением).
     5. Подсистема должна предоставлять возможность формирования и отображения «Карточки пользователя», включающей в себя: общую информацию по выбранному пользователю (с возможностью добавления дополнительных полей), используемые им учетные записи из Active Directory, его контактные данные (e-mail адреса, учетные записи IM-клиентов), а также информацию по связям текущего пользователя за указанный период времени.
     6. Подсистема должна предоставлять возможность просмотра информации по активности сотрудников в режиме реального времени с возможностью фильтрации по категориям активности пользователя.
     7. Подсистема должна обеспечивать возможность оперативного контроля за происходящим на рабочих местах пользователей в режиме реального времени: просмотр происходящего на экранах мониторов, прослушивание речи сотрудников, просмотр происходящего за компьютером посредством подключенной веб-камеры.
     8. Подсистема должна предоставлять возможность генерации отчетов по имеющимся базовым шаблонам, а также предусматривать возможность добавления пользовательских шаблонов.
     9. Подсистема должна поддерживать предоставление отчетов в табличном, диаграммном, в виде временного графика, а также в виде интерактивного графа связей с возможностью фильтрации событий по различным метрикам.
     10. Подсистема должна производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности.
     11. Подсистема должна отображать информацию по активности пользователей в запускаемых ими приложениях в течение рабочего дня. При нарушениях сотрудниками установленного в компании трудового распорядка (поздний приход, ранний уход, недостаточная активность; длительная работа в приложениях, не связанных с рабочей деятельностью), должна быть предусмотрена возможность формирования оповещения по данному факту с последующей отправкой его на электронный адрес сотрудника службы информационной безопасности.
     12. Подсистема должна генерировать краткие и детальные отчеты по продуктивности работы пользователей за выбранный период времени.
     13. Подсистема должна генерировать отчеты по устройствам: перечень установленного оборудования на компьютерах пользователей и отчет по изменениям в устройствах (комплектующих) компьютеров.
     14. Подсистема должна отображать:
   * операции с агентами/протоколами, совершенные любым либо указанным пользователем;
   * список компьютеров с нерабочими агентами;
   * список компьютеров без агентов;
   * информацию о количестве сообщений по выбранным компьютерам за заданный промежуток времени.
     1. Подсистема должна предоставлять возможность быстрого перехода к поиску и просмотру найденных документов.
     2. Подсистема должна предоставлять возможность переходов по связанным отчетам.
     3. Подсистема должна предусматривать представление связей между внутренними и внешними адресатами в виде интерактивного графа для получения наглядного представления о круге общения выбранного пользователя или нескольких пользователей, выявления общих контактов для данных пользователей, а также контактов внешних адресатов с сотрудниками компании.
     4. Подсистема должна обеспечивать получение наглядного представления об адресах, с которых выбранный пользователь отправлял либо на которые получал сообщения.
     5. Подсистема должна предусматривать возможность конвертации сгенерированных отчетов в PDF-файл, равно как и вывод их на печать.
   1. **Требования к подсистеме принятия решений**
      1. Подсистема должна иметь изолированное разграничение прав доступа.
      2. Подсистема должна выносить единый вердикт (инцидент / не инцидент) для каждого перехваченного объекта.
      3. Подсистема должна предоставлять возможности для ведения журнала инцидентов с возможностью рубрикации по каналам передачи данных, протоколам, пользователям, правилам проверки.
      4. Подсистема должна предоставлять возможность уведомления ответственных лиц об инцидентах по электронной почте.
      5. Подсистема должна предоставлять возможности для задания правил автоматического вынесения вердикта по объекту (инцидент / не инцидент). Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:
   * формальных признаков перехваченного объекта (доменное имя, отправитель, получатель, хост, размер, расширение файла, канал передачи данных, протокол и т.д.);
   * защищенных паролем архивов;
   * результатов контентного анализа текста, извлеченного из перехваченных объектов (по словам и образцам текстов, тематическим словарям, путем сравнения с базой эталонных документов, путем поиска текстов, близких по смыслу или содержанию с эталоном, поиска алфавитно-цифровых объектов, а также поиска с использованием регулярных выражений).
   * результатов анализа графических объектов (сканы паспортов, кредиток, схем, чертежей и т.д.) без использования технологии OCR
   * результатов анализа информации, содержащейся в эталонной выгрузке БД с возможностью создания логических условий поиска по комбинациям строк и столбцов
   * результатов анализа документов с печатями различных подразделений
     1. Подсистема должна предоставлять возможности для изменения существующих и применения новых правил автоматического вынесения вердикта (правил проверки).
     2. Подсистема должна предоставлять возможность выполнения ретроспективного контроля перехваченных документов.
     3. Подсистема должна предусматривать возможность объединения политик безопасности (правил проверки) в группы.
     4. Подсистема должна предоставлять возможность задания для каждой группы политик безопасности индивидуальных настроек: перечня источников данных, по которым будет проводиться опрос, расписания проверки, списка получателей оповещений об инцидентах, списка исключений.
     5. Подсистема должна предоставлять возможность экспорта/импорта структуры настроек.
     6. Подсистема должна предоставлять возможность добавления пользователей и наделения их правами просмотра и редактирования тех или иных политик безопасности и списков исключений, в том числе возможность выставления запрета на данные действия.
     7. Подсистема должна предоставлять возможности протоколирования выявленных инцидентов.
     8. Подсистема должна поддерживать возможность категоризации инцидентов с помощью цветовых меток.
     9. Подсистема должна поддержать возможность экспорта данных об инцидентах и событиях посредством syslog.
     10. Подсистема должна предоставлять возможность подбора паролей для перехваченных архивов, защищенных паролем. База (словарь) для перебора паролей генерируется автоматически на базе данных модуля контроля данных, вводимых с клавиатуры.
     11. Подсистема должна предоставлять возможности для принятия решений в отношении следующих типов объектов:
   * сообщений, переданных по поддерживаемым Системой каналам и протоколам;
   * файлов форматов: MS Office (doc, docx, dot, xls, xlsx, xlsb, xlsm, xlt, xltx, xltm, ppt, pptx, rtf, pot, vsd, vst, vsdx), Open Office (sxw, stw, odt, ods), HTML-файлы (htm, html, shtml, mht, css, js, maff), файлы почтовых сообщений (eml, msg), базы данных (mdb), дополнительные форматы документов (txt, xml, pdf, djvu, csv, lst, log, bat, ini, wri);
   * распознанных и проанализированных текстов в графических файлах форматов bmp, jpg, jpeg, png, tif, tiff, gif;
   * документов, вложенных в сжатые файлы: rar, zip, 7z, jar, tar, arj, gz, gzip, cab, iso, chm, hlp, 001.
     1. Подсистема должна обеспечить наличие следующих возможностей обнаружения критичной информации:
   * по ключевым словам, в том числе с возможностью ограничений по взаимному расположению искомых слов и с учетом морфологических особенностей и синонимии русского языка;
   * возможность обнаружения похожих документов на основе образца, схожего по содержанию с искомым;
   * по формальным признакам сообщений и файлов (доменный пользователь, имя компьютера, отправитель, получатель, размер, имя файла, формат и др.), в том числе для файлов, из которых не может быть извлечен текст;
   * по заранее заданному словарю с целью выявления определенных типов документов (резюме, финансовые и бухгалтерские отчеты);
   * возможность создания комплексных поисковых запросов, включающих в себя несколько критериев (фразовый поиск, поиск по абзацам и целым документам и атрибутам), объединенных логическими операторами AND, OR, NOT;
   * по регулярным выражениям PCRE – поиск сложных алфавитно-цифровых объектов (номера паспортов, индивидуальные номера налогоплательщиков, номера кредитных карт, договоров или счетов, кодов классификаторов и т.п.), с возможностью создания комплексных регулярных выражений (состоящих из нескольких простых), задания порога срабатывания по суммарному количеству регулярных выражений, количеству вхождений регулярного выражения в документ и количеству промежуточных символов между регулярными выражениями, возможностью использования как стандартных выражений, включенных в дистрибутив, так и создание пользовательских, а также с возможностью проверки полученных результатов;
   * по цифровым отпечаткам конфиденциальных документов, с возможностью указания порога срабатывания;
   * по значениям атрибутов (как общих атрибутов, так и уникальных для отдельных каналов связи);
     1. Подсистема должна предусматривать наличие нескольких встроенных словарей.
     2. Подсистема должна обеспечивать устойчивость к следующим видам манипуляции с информацией:
   * импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными;
   * изменение порядка слов;
   * изменения расстояний между словами;
   * изменение форматирования документа;
   * изменение словоформ;
   * замены букв на символы другого алфавита;
   * использование цифр вместо букв;
   * изменение расширений файлов.
     1. Подсистема должна предоставлять возможности для просмотра детальной информации по каждому инциденту.
4. **Требования к подсистеме контроля**
   1. **Общие требования к функциям Агента для ОС Windows**
      1. **Требования к модулю контроля электронной почты**
         1. Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, MAPI, HTTP (веб-почта: как исходящая, так и входящая), при помощи почтовых клиентов или браузеров. Модуль должен иметь подключаемую функцию автоматической остановки исходящих почтовых сообщений по протоколам SMTP и HTTP, а также блокировки исходящих электронных сообщений, передаваемых с помощью почтового клиента Outlook по протоколам IMAP и MAPI, на основе контентного и/или контекстного анализа как почтовых сообщений, так и вложений.
         2. Модуль должен предоставлять возможность блокировки исходящей почты по контентным и/или контекстным критериям на почтовом сервере с возможностью работы в разрыв.
         3. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.
      2. **Требования к модулю контроля сервисов обмена мгновенными** сообщениями
         1. Модуль должен обеспечивать контроль:
   * входящих/исходящих сообщений и файлов, переданных пользователями по протоколам:
     + OSCAR (ICQ/QIP),
     + XMPP (Cisco Jabber),
     + MMP (Агент Mail.ru);
   * входящих и исходящих сообщений по протоколу HTTP в социальных сетях:
     + Facebook,
     + LinkedIn,
     + ВКонтакте,
     + Moй [Мир@Mail.ru](mailto:Мир@Mail.ru),
     + Одноклассники.ru,
   * чатов, файлов, переданных при помощи desktop-версий мессенджеров:
     + Skype,
     + Lync,
     + Viber,
     + Telegram,
     + WhatsApp,
     + Rocket.chat,
   * чатов, файлов веб-версий мессенджеров:
     + Skype (web.skype.com),
     + Telegram (web.telegram.org),
   * чатов, звонков и файлов, переданных при помощи:
     + Zoom Chat,
     + TrueConf Client,
     + конференций Zoom;
   * сообщений и файлов ресурса slack.com.
     + 1. Модуль должен осуществлять контроль сеансов текстовой и голосовой связи, файлов при помощи Skype.
       2. Модуль должен обеспечивать контроль входящих/исходящих сообщений, файлов коммуникационных программ-клиентов Microsoft Lync, Viber и Telegram.
       3. Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.
       4. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др.
     1. **Требования к модулю контроля FTP-соединений**
        1. Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединения, в том числе с применением SSL-шифрования.
        2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.
        3. Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище.
     2. **Требования к модулю контроля HTTP-трафика**
        1. Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).
        2. Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome; Edge.
        3. Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.
        4. Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).
        5. Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.
        6. Модуль должен обеспечивать вычитку сохраненных в браузерах авторизационных данных пользователей к интернет-ресурсам, а также позволять осуществление подбора мастер-пароля в случаях, если данные защищены.
        7. Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков, а также использование категорий сайтов для блокировки и/или разрешения посещения интернет-ресурсов, предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу.
        8. Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту.
        9. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.
     3. **Требования к модулю контроля печати**
        1. Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров.
        2. Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов.
        3. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др.
     4. **Требования к модулю контроля съёмных устройств**
        1. Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (СD-/DVD-приводы, съемные накопители USB и FireWire, USB-устройства, Wi-Fi и Bluetooth) и портам (USB, FireWire, COM, LPT, IRDA + IDE/SATA, Serial Port, Parallel Port, PCI, SCSI и прочее).
        2. Модуль должен поддерживать работу в терминальной сессии.
        3. Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.
        4. Модуль должен предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство.
        5. Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве.
        6. Модуль должен предоставлять возможность теневого копирования данных, передаваемых через буфер обмена, в том числе буфер обмена RDP-сессии.
        7. Модуль должен предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе.
        8. Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».
        9. Модуль должен предоставлять возможность блокировки записи на подключаемые внешние USB-устройства, исходя из формальных признаков файлов (имя файла, формат), а также по содержимому передаваемых данных.
        10. Модуль должен предоставлять возможность запрета копирования данных, передаваемых через RDP-сессию.
        11. Модуль должен позволять ограничение установки RDP-подключения как на удаленные рабочие станции или серверы, так и на рабочую станцию или сервер с работающим модулем.
        12. Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя.
        13. Модуль должен предоставлять возможность блокировки Bluetooth-устройств и сервисов.
        14. Модуль должен предоставлять возможность контроля буфера обмена на компьютере пользователя, а также блокировку передачи данных через буфер обмена по содержимому копируемых данных.
        15. Модуль должен предоставлять возможность использования «белых списков» устройств, к которым в дальнейшем пользователь будет иметь неограниченный доступ либо доступ «только чтение», а также «черных списков» устройств, доступ к которым будет заблокирован.
        16. Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.
     5. **Требования к модулю контроля событий на мониторах и действий сотрудников**
        1. Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции и/или при вводе пользователем ключевых слов.
        2. Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, звонке
        3. Модуль должен обеспечивать видеозапись происходящего на экранах мониторов согласно настроенному расписанию или событиям, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции и/или при вводе пользователем ключевых слов.
        4. Модуль должен обеспечивать создание снимков, видеозаписи посредством подключенной к рабочей станции веб-камеры по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции, с возможностью использования нескольких веб-камер.
        5. Модуль должен позволять скорректировать расписание создания снимков при посещении определенных (настроенных заранее) интернет-узлов, авторизации в операционной системе, отсутствии пользовательских сессий.
        6. Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи.
        7. Модуль должен обеспечивать одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени.
        8. Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры в режиме реального времени.
        9. Модуль должен предоставлять возможность экспорта перехваченных снимков экрана и видеозаписей в отдельную папку.
        10. Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.
        11. Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.
        12. Модуль должен обеспечивать возможность блокировки нажатий клавиши «PrintScreen».
        13. Модуль должен выделять и позволять исключать из аудита набранные символы, если они являются вводом пароля для всех случаев, когда это технически возможно.
        14. Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.
        15. Модуль должен предоставлять возможность поиска, вводимого с клавиатуры или помещаемого в буфер обмена содержимого за определенный период времени применительно к заданным пользователям, компьютерам, именам запущенных процессов, MAC- и IP-адресам, продолжительности работы в приложении.
     6. **Требования к модулю контроля разговоров сотрудников**
        1. Модуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.), а также иметь возможность аудиозаписи с выхода звуковой карты.
        2. Модуль должен предусматривать возможность активации записи голосов по расписанию, при запуске определенных процессов, внутри офиса/за его пределами (в командировке), при отсутствии авторизованных пользователей в операционной системе, автоматической активации микрофона при деактивации его пользователями в настройках ОС, а также возможность настройки качества записываемого звукового файла.
        3. Модуль должен обеспечивать помещение записанных звуковых файлов в базу данных либо использовать для хранения бинарных данных файловое хранилище.
        4. Модуль должен предоставлять возможность экспорта перехваченных разговоров в отдельную папку.
     7. **Требования к модулю контроля активности пользователей и приложений**
        1. Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.
        2. Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.
        3. Модуль должен иметь подключаемую возможность автоматической категоризации любых посещенных сайтов на тематические группы, используя заранее загруженную и регулярно пополняемую базу классификации сайтов.
     8. **Требования к модулю контроля облачных хранилищ данных**
        1. Модуль должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов:
   * Google Drive,
   * OneDrive,
   * Office 365,
   * DropBox,
   * Evernote,
   * Яндекс.Диск,
   * iCloud,
   * DropMeFiles,
   * OwnCloud,
   * SharePoint,
     + 1. Модуль должен обеспечивать контроль файлов, передаваемых в программах удаленного доступа:
   * TeamViewer,
   * AnyDesk
     + 1. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др.
       2. Модуль должен обеспечивать возможность блокировки передачи в облачные хранилища посредством веб-браузера файлов, соответствующих определенному контенту и/или контексту, за исключением трафика вне спецификации HTTPS.
   1. **О**б**щие требования к функциям Агента для ОС Linux**
      1. **Требования к модулю контроля электронной почты**
         1. Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, HTTP (веб-почта: как исходящая, так и входящая) при помощи любых почтовых клиентов или браузеров. Иметь подключаемую функцию автоматической остановки исходящих почтовых сообщений по протоколам SMTP, на основе контентного и/или контекстного анализа как почтовых сообщений, так и вложений.
         2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.
      2. **Требования к модулю контроля сервисов обмена мгновенными сообщениями**
         1. Модуль должен обеспечивать контроль:
   * входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), XMPP (Jabber, Google Hangouts), MMP (Агент Mail.ru), SIP (X-Lite и др.) и др.;
   * входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Moй Мир@Mail.ru, Одноклассники.ru, Google+, Мамба.ru и прочее);
     + 1. Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.
       2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др.
     1. **Требования к модулю контроля FTP-соединений**
        1. Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединение, в том числе с применением SSL-шифрования.
        2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.
     2. **Требования к модулю контроля HTTP-трафика**
        1. Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).
        2. Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Mozilla Firefox; Opera; Google Chrome.
        3. Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.
        4. Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).
        5. Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.
        6. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.
     3. **Требования к модулю контроля печати** 
        1. Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров.
        2. Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов.
        3. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др.
        4. Модуль должен поддерживать возможность исключения из контроля отдельных принтеров (в том числе по их описанию и месту расположения), пользователей.
     4. **Требования к модулю контроля и управления доступом съёмных устройств** 
        1. Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (съемные накопители USB, Wi-Fi и сетевым папкам, модемам и сетевым адаптерам).
        2. Модуль должен поддерживать работу в терминальной сессии.
        3. Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.
        4. Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве или записываемых на внешнее USB-устройство.
        5. Модуль должен предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство через буфер обмена, в том числе буфер обмена RDP-сессии.
        6. Модуль должен предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе.
        7. Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».
        8. Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.
     5. **Требования к модулю контроля событий на мониторах и действий сотрудников** 
        1. Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции.
        2. Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи.
        3. Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.
        4. Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.
        5. Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.
     6. **Требования к модулю контроля разговоров сотрудников** 
        1. Модуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.).
        2. Модуль должен предусматривать возможность активации записи голосов по расписанию, внутри офиса/за его пределами (в командировке), а также возможность настройки качества записываемого звукового файла.
     7. **Требования к модулю контроля активности пользователей и приложений** 
        1. Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях.
        2. Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.
     8. **Требования к модулю контроля облачных хранилищ данных** 
        1. Модуль должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов Google Drive, Google Docs, OneDrive, SkyDrive, Office 365, DropBox, Evernote, Яндекс.Диск, Cloud.mail.ru, Amazon S3, iCloud, DropMeFiles, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia, My-Files, Nextcloud, Seafile, SharePoint, Acronis File Advanced, Cloudian S3 storage, Disk Bitrix24.
        2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др.
   1. **Общие требования к функциям Агента для ОС MacOS**
      1. **Требования к модулю контроля событий на мониторах и действий сотрудников**
         1. Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции.
         2. Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи.
         3. Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.
         4. Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.
         5. Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.
      2. **Требования к модулю контроля активности пользователей и приложений**
         1. Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях.
         2. Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.
   2. **Требования к функциям контроля данных на уровне сетевого перехвата (при интеграции с прокси-сервером (по протоколу ICAP) либо сетевым оборудованием через зеркалирование трафика (SPAN))**
      1. **Требования к модулю контроля электронной почты**
         1. Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, HTTP (веб-почта: как исходящая, так и входящая), при помощи почтовых клиентов или браузеров. При этом нешифрованный трафик HTTP доступен в как в режиме зеркалирования, так и в режиме интеграции с прокси-сервером. Нешифрованный SMTP, POP3 и IMAP трафик доступен только в режиме зеркалирования. Шифрованный HTTP(S) трафик доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата.
         2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.
      2. **Требования к модулю контроля сервисов обмена мгновенными сообщениями**
         1. Модуль должен обеспечивать контроль в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата:
   * входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Moй Мир@Mail.ru, Одноклассники.ru, Google+, Мамба.ru и других, на усмотрение Разработчика Системы);
   * чатов, файлов веб-версии Skype (web.skype.com);
   * чатов, файлов веб-версий мессенджеров: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost;
   * истории передачи файлов и чатов Instagram, VK Teams;
   * сообщений и файлов ресурса slack.com.
     + 1. Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, передаваемых по протоколу HTTP в социальных сетях и веб-мессенджерами (Rocket.chat, Mattermost и др.), соответствующих определенному контексту.
       2. Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.
       3. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др.
     1. **Требования к модулю контроля FTP-соединений**
        1. Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединения, в том числе с применением SSL-шифрования в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата
        2. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.
        3. Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище.
     2. **Требования к модулю контроля HTTP-трафика**
        1. Контроль защищенного HTTPS трафика может быть доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата.
        2. Контроль незащищенного HTTP трафика может быть доступен как режиме интеграции с прокси-сервером, так и в режиме зеркалирования трафика.
        3. Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).
        4. Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome.
        5. Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).
        6. Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.
        7. Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков, а также использование категорий сайтов для блокировки и/или разрешения посещения интернет-ресурсов, предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу.
        8. Модуль должен обеспечивать возможность блокировки передачи запросов, соответствующих определенному контексту.
        9. Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

**БАНКОВСКИЕ РЕКВИЗИТЫ**

**для внесения ГОКЗ и ГОИД**

|  |  |  |
| --- | --- | --- |
| **Для зачисления Кыргызских сомов** | | **For transfer of US dollars** |
| **Intermediary Bank**  **(Банк-посредник)** |  | **Kookmin Bank, Seoul, South Korea**  **SWIFT: CZNBKRSE** |
| **Bank of Beneficiary**  **(Банк получателя)** | ОАО “Айыл Банк”,  г. Бишкек, Кыргызская Республика | **OAO AIYL BANK, Kyrgyz Republic, Bishkek**  **SWIFT: AIYLKG22**  **Номер счета: 7C78USD013** |
| **Beneficiary (Получатель)** | ЗАО "Альфа Телеком",  Счет № 1350100027537623  БИК: 135001 | **Beneficiary Name: CJSC Alfa Telecom**  **Beneficiary account: NO.1350100022480485**  **Address: KYRGYZSTAN, Bishkek, Suyumbaeva 123** |
| **Purpose of payment**  **(Назначение платежа)** | ***- Гарантийное обеспечение конкурсной заявки;***  ***- Гарантийное обеспечение исполнения договора от \_\_\_\_ №\_\_\_\_;*** | **В назначении указать: за что, р/счет и наименование компании.**  **Например**: Account replenishment, FOR FURTHER CREDIT TO ACCOUNT. NO.1350100022480485 CJSC Alfa Telecom USD |

**Примечание:** Расходы, связанные с банковским переводом, несет победитель конкурса.

**Приложение 2 к Приглашению**

**Форма**

|  |  |
| --- | --- |
|  | **КОНКУРСНАЯ ЗАЯВКА**  КОМУ: **ЗАО «Альфа Телеком»**  На Приглашение № \_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г.  ОТ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(наименование поставщика)*  **Для резидентов КР:** |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Наименование товара, Подробное описание** | **Кол-во** | **Цена**  **за ед. без НДС\*** | **Общая стоимость, без НДС\*** | **Сумма**  **НДС\*** | **Общая стоимость, с учетом НДС\*** | | **Услуги по внедрению DLP системы** (прописать подробную техспецификацию, модель и т.д.) | 400 |  |  |  |  | | **Итого:** | | | | |  |   **Для нерезидентов КР:**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Наименование товара, Подробное описание** | **Кол-во** | **Цена**  **за ед.** | **Общая стоимость, без НДС\*** | **Общая стоимость** | | **Услуги по внедрению DLP системы** (прописать подробную техспецификацию, модель и т.д.) | 400 |  |  |  | | **Итого:** | | | |  |   **Срок поставки составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рабочих дней**    **Срок технической поддержки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ месяцев**    В цену, указанную поставщиком, должны быть включены все налоги, сборы и другие платежи, взимаемые в соответствии с законодательством Кыргызской Республики, накладные затраты, транспортные и другие затраты поставщика.  **\*Сумма НДС в графах заполняется поставщиком, только в случае если он является плательщиком НДС в Кыргызской Республике на момент подачи конкурсной заявки.**  Данная конкурсная заявка действительна в течение 60 (шестидесяти) календарных дней с даты вскрытия конкурсных заявок.  Подавая настоящую конкурсную заявку, выражаем свое согласие заключить договор (в случае признания конкурсной заявки, выигравшей) на условиях, обозначенных в Требованиях к закупке и по форме Договора согласно приложению 3 к Приглашению.  В случае принятия нашей Конкурсной заявки, мы обязуемся предоставить гарантийное обеспечение исполнения Договора на сумму \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, для надлежащего выполнения Договора и в сроки, указанные в Конкурсной документации.  Также подавая конкурсную заявку подтверждаем и гарантируем свою правоспособность, наличие регистрации в установленном законодательством порядке, а также наличие необходимых разрешительных документов на осуществление нашей деятельности. Гарантируем, что лицо, подписавшее настоящую конкурсную заявку, обладает всеми необходимыми полномочиями на ее подписание. | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО) (должность) (подпись и печать)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2022 года

(дата заполнения)

**Приложение № 2.1 к Приглашению**

**Форма для заполнения соответствия техническим требованиям**

**(прописать по каждой позиции согласно существенных требований/технических спецификаций)**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование требований** | **Соответствует/Не соответствует** | **Примечание** |
| **1.** | **Требования к поставке лицензионных программных средств** |  |  |
| 1.1. | Дистрибутив программного обеспечения должен поставляться с документацией в электронном или печатном виде на русском языке. Документация должна включать в себя правила установки и использования лицензионного программного обеспечения. |  |  |
| 1.2. | Исполнитель должен предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие права на обновление и поддержку (гарантийное сопровождение) программного обеспечения в течение 12 (двенадцати) месяцев. |  |  |
| 1.3. | Лицензии системы должны позволять осуществлять одновременный контроль не менее 400 пользователей. |  |  |
| 1.4. | Подсистемы контентного анализа и принятия решений должны лицензироваться за единицы (одна лицензия на каждую подсистему). |  |  |
| 1.5. | Модули подсистемы контроля должны иметь лицензирование по конечным пользователям, то есть одна лицензия требуется для одной подконтрольной (защищаемой Системой) доменной или локальной учетной записи. |  |  |
| 1.6. | Лицензии модулей подсистемы контроля должны быть конкурентными. Это значит, что одну лицензию можно использовать для контроля разных пользователей (учетных записей) только в разные периоды времени. |  |  |
| 1.7. | Программное обеспечение должно условно состоять из следующих модулей или подсистем: |  |  |
| 1.7.1. | Подсистема контроля, состоящая из: |  |  |
| • | модуль контроля электронной почты |  |  |
| • | модуль контроля сервисов обмена мгновенными сообщениями |  |  |
| • | модуль контроля FTP-соединений |  |  |
| • | модуль контроля HTTP-трафика (POST- и GET-запросы) |  |  |
| • | модуль контроля печати |  |  |
| • | модуль контроля и управления доступом съёмных устройств |  |  |
| • | модуль контроля событий на мониторах и действий сотрудников |  |  |
| • | модуль контроля разговоров сотрудников (аудиоконтроль) |  |  |
| • | модуль контроля активности пользователей и приложений |  |  |
| • | модуль контроля облачных хранилищ данных |  |  |
| 1.7.2. | Подсистема контентного анализа |  |  |
| 1.7.3. | Подсистема принятия решений |  |  |
| **2.** | **Технические требования к Системе** |  |  |
| **2.1.** | **Требования к Системе в целом** |  |  |
| 2.1.1. | Программное обеспечение для защиты информации (Далее – Система) должно обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей. Система должна поддерживать работу на уровне рабочих станций (Endpoint), на уровне сети (получение теневой копии трафика от сетевого оборудования либо прокси-сервера) и на уровне интеграций со сторонними системами (пр. технологий - SMTP, ICAP, API). Система должна предоставлять возможность работы в одном или нескольких перечисленных режимах одновременно. |  |  |
| 2.1.2. | Система должна быть построена на базе клиент-серверной архитектуры, где сервер выполняет роли администрирования, обработки, хранения и анализа данных, а клиент выполняет роль пользовательского интерфейса или агента. |  |  |
| 2.1.3. | Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Windows: |  |  |
| • | Windows 7 x32/x64; |  |  |
| • | Windows 8, 8.1 x32/х64; |  |  |
| • | Windows 10 x32/х64; |  |  |
| • | Windows 11 х64; |  |  |
| • | Windows Server 2008 R2; |  |  |
| • | Windows Server 2012, 2012 R2; |  |  |
| • | Windows Server 2016; |  |  |
| • | Windows Server 2019. |  |  |
| 2.1.4. | Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Linux: |  |  |
| • | Ubuntu 16.04 x32/x64, 18.04 x64, 20.04 x64, 21.04 x64. |  |  |
| • | CentOS 7.4 x64, 8 x64; |  |  |
| • | Red Hat Enterprise Linux (RHEL) 7 x64; |  |  |
| • | AltLinux 9 x32/x64; |  |  |
| 2.1.5. | Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства MacOS: |  |  |
| • | Mojave 10.14; |  |  |
| • | Catalina 10.15 |  |  |
| • | Big Sur 11.0.1; |  |  |
| • | Monterey 12.1. |  |  |
| 2.1.6. | Система должна иметь потенциал развития и поддержки новых версий популярных версий операционных систем. |  |  |
| 2.1.7. | В связи с существенной разницей архитектур операционных систем Windows, Linux, MacOS допускается разница между функциями Агента, реализованными для ОС Windows, Linux и MacOS, а также между разными ядрами или версиями ОС Linux. |  |  |
| 2.1.8. | Все серверные функции Системы должны выполняться в рамках единого решения, СУБД одной версии для архивирования данных и поддерживать установку на операционных системах семейства Windows Server/Linux Server. |  |  |
| 2.1.9. | Система должна поддерживать работу в замкнутом контуре, то есть в локальной сети Заказчика без выхода в сеть Интернет. Исключением служат отдельные опциональные функции в явном виде требующие интернет-соединения). |  |  |
| 2.1.10. | Все сетевые соединения, протоколы связи и направления соединений должны быть указаны в технической документации на Систему. |  |  |
| 2.1.11. | Система должна обеспечивать защиту данных, передаваемых агентскими или клиентскими компонентами по линиям связи. |  |  |
| 2.1.12. | Система должна не оказывать негативного влияния либо ухудшать основные функциональные характеристики Сети заказчика (надежность, быстродействие, возможность изменения конфигурации, удобство использования); |  |  |
| 2.1.13. | Система должна обладать характеристиками масштабирования и отказоустойчивости; |  |  |
| 2.1.14. | Система должна обеспечить интеграцию в существующую у Заказчика вычислительную сеть без изменения топологии сети; |  |  |
| 2.1.15. | Система должна предполагать возможность установки отдельного модуля по каждому или группе контролируемых каналов передачи данных; |  |  |
| 2.1.16. | Система должна предполагать возможность выборочной активации модулей контроля для вышеперечисленных каналов передачи данных. |  |  |
| 2.1.17. | Система должна иметь удобный и понятный пользовательский интерфейс, где все сообщения и документация должны быть на русском языке; |  |  |
| 2.1.18. | Система не должна оказывать негативного влияния на нормальное функционирование серверов и рабочих станций Заказчика; |  |  |
| 2.1.19. | Система должна обеспечивать разграничение прав доступа к перехваченной информации, политикам безопасности и настройкам системы; |  |  |
| 2.1.20. | Система должна обеспечивать контроль веб-трафика на уровне рабочих станций, на уровне интеграций с прокси-серверами по протоколу ICAP и на уровне передачи теневой копии трафика (SPAN) с сетевых шлюзов; |  |  |
| 2.1.21. | Система должна обеспечивать контроль почтового трафика как на уровне рабочих станций, так и на уровне интеграции с корпоративным почтовым сервером; |  |  |
| 2.1.22. | Система должна обладать возможностью оптимизации нагрузки на ресурсы территориально разделенных сетей с «узким» каналом передачи данных благодаря предварительному сжатию информации или настройке расписания и скорости ее передачи; |  |  |
| 2.1.23. | Система должна обеспечивать индексирование документов, перехваченных модулями контроля, для ускорения поиска и обработки событий; |  |  |
| 2.1.24. | Система должна интегрироваться с Active Directory. |  |  |
| 2.1.25. | Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах ОС Windows. |  |  |
| 2.1.26. | Система должна иметь веб-интерфейс при работе с результирующими отчетами Системы, при этом разграничение доступа должно быть централизованным и индивидуальным в веб-интерфейсе. |  |  |
| 2.1.27. | Для информационного обмена между компонентами системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet). |  |  |
| 2.1.28. | Система должна обеспечивать блокировку HTTP(S)-трафика на рабочих станциях согласно настраиваемым атрибутивно-зависимым правилам. Тематическая категория блокируемого HTTP(S) ресурса также должна являться атрибутом. |  |  |
| 2.1.29. | Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах ОС Windows для всех указанных в п. 2.1.3 операционных систем. |  |  |
| 2.1.30. | Агент Системы, осуществляющий контроль на уровне рабочих станций c ОС Windows, должен быть подписан цифровой подписью. |  |  |
| 2.1.31. | Подсистема контентного анализа должна предоставлять возможности: |  |  |
| • | проведения ретроспективного анализа архива информации; |  |  |
| • | генерации отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности; |  |  |
| • | просмотра активности пользователей в режиме реального времени. |  |  |
| 2.1.32. | Подсистема принятия решений должна предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту – нарушает или не нарушает он существующие правила. |  |  |
| 2.1.33. | Модуль контроля электронной почты должен обеспечивать контроль сообщений электронной почты (протоколы SMTP/ESMTP/SMTPS, POP3/POP3S, IMAP, MAPI), а также иметь подключаемую функцию автоматической остановки отправки сообщения в случае возникновения инцидента, зарегистрированного данным модулем на конечных станциях или посредством интеграции с почтовым сервером. |  |  |
| 2.1.34. | Модуль контроля сервисов обмена мгновенными сообщениями должен обеспечивать контроль сообщений и файлов, переданных при помощи популярных интернет-мессенджеров. В частности, обеспечивать контроль сеансов текстовой связи, файлов, переданных посредством Skype, контроль чатов, звонков и файлов коммуникационных клиентов Microsoft Lync, Viber, Telegram и Zoom Chat, Whatsapp и др.. |  |  |
| 2.1.35. | Модуль контроля FTP-соединений должен обеспечивать контроль входящего и исходящего FTP-трафика. В случае контроля на уровне рабочих станций также необходима поддержка FTP через SSL (FTPS). |  |  |
| 2.1.36. | Модуль контроля HTTP-трафика должен обеспечивать контроль POST-запросов при использовании пользователями интернет-сервисов, а также иметь подключаемую функцию автоматической остановки трафика в случае возникновения инцидента, зарегистрированного данным модулем. |  |  |
| 2.1.37. | Модуль контроля печати должен обеспечивать контроль документов, отправленных на печать при помощи сетевых или локальных принтеров. |  |  |
| 2.1.38. | Модуль контроля и управления доступом съемных устройств должен обеспечивать контроль файлов, записываемых на USB-устройства, CD/DVD и др. типы съемных устройств. |  |  |
| 2.1.39. | Модуль контроля событий на мониторах и действий сотрудников должен обеспечивать контроль изображений с экранов пользователей, предоставлять возможность осуществления видеозаписи действий, создания снимков и записи видео посредством веб-камеры, а также предоставлять возможность просмотра содержимого мониторов и действий пользователей за рабочей станцией в режиме реального времени. Модуль должен осуществлять контроль данных, вводимых с клавиатуры, логирование нажатий клавиш в любых приложениях (в том числе нажатия системных клавиш и их сочетаний). В целях обеспечения конфиденциальности, модуль, при наличии технической возможности, должен выделять ввод пароля и давать возможность исключить пароли из аудита. |  |  |
| 2.1.40. | Модуль контроля разговоров сотрудников должен обеспечивать аудиозапись разговоров с помощью подключенного к рабочей станции микрофона. В целях обеспечения конфиденциальности третьей стороны важно, чтобы модуль позволял выбирать различные настройки своей работы для случаев, когда сотрудник находится в офисе и за его пределами. |  |  |
| 2.1.41. | Модуль контроля активности пользователей и приложений должен обеспечивать мониторинг активности пользователей и запускаемых ими процессов с учетом длительности в течение рабочего дня. |  |  |
| 2.1.42. | Модуль контроля облачных хранилищ данных должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов (Google Drive, OneDrive, Office 365, Dropbox, Evernote, Яндекс Диск, cloud.mail.ru и др.), а также позволять контролировать файлы, передаваемые в программах удаленного доступа (TeamViewer, VNC, Radmin, LiteManager). |  |  |
| 2.1.43. | В Системе должны быть реализованы функции, обеспечивающие управление настройками конфигурации Системы и осуществляющие автоматизированный контроль штатного функционирования Системы. Под управлением понимается комплекс действий, позволяющих сотрудникам Заказчика изменять заданные настройки Системы самостоятельно, без привлечения сторонних специалистов. Под автоматизированным контролем штатного функционирования подразумевается мониторинг штатной работы всех компонентов Системы и автоматическое уведомление администратора в случае нештатных ситуаций. |  |  |
| **2.2.** | **Требования к способам и средствам связи для информационного обмена** |  |  |
| 2.2.1. | Система должна функционировать в составе информационно-вычислительной сети Заказчика. |  |  |
| 2.2.2. | Модули контроля на уровне рабочей станции должны иметь возможность использования HTTPS для передачи данных на сервер Системы для защиты соединения и/или использовать альтернативные алгоритмы шифрования передаваемых данных. |  |  |
| 2.2.3. | Система должна корректно работать в сетях с Active Directory. |  |  |
| 2.2.4. | Система должна поддерживать работу в виртуальной инфраструктуре. |  |  |
| 2.2.5. | Для информационного обмена между компонентами Системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet). |  |  |
| 2.2.6. | Для информационного обмена между Системой и корпоративной почтовой системой должен использоваться протокол SMTP. |  |  |
| 2.2.7. | Система должна предоставлять возможность однозначного определения данных сотрудника компании, отправившего информацию, благодаря интеграции с Active Directory: |  |  |
| • | учетной записи пользователя, |  |  |
| • | информации об использованной рабочей станции (имени, IP- и MAC-адреса). |  |  |
| **2.3.** | **Требования по диагностированию Системы** |  |  |
| 2.3.1. | Система должна обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности. |  |  |
| 2.3.2. | Каждый модуль Системы должен иметь штатный и расширенный режим записи в журналы. В случае программных сбоев должен быть предусмотрен отладочный режим принудительной записи в системные журналы. Отладочный режим включается автоматически без участия пользователя при наступлении программного сбоя. |  |  |
| 2.3.3. | В случае многопользовательской работы модуль должен автоматически создавать раздельные журналы для каждого пользователя. |  |  |
| **2.4.** | **Перспективы развития и модернизации Системы** |  |  |
| 2.4.1. | Система должна допускать наращивание производительности за счет улучшения характеристик технических средств. |  |  |
| 2.4.2. | Система должна обеспечивать возможность модернизации путем замены технического и/или программного обеспечения. |  |  |
| 2.4.3. | Исполнитель может привлекаться для консультаций Заказчика для согласования минимально достаточного или рекомендуемого оборудования при планировании внедрения Системы. |  |  |
| **2.5.** | **Требования к функциям администрирования** |  |  |
| 2.5.1. | Интерфейс администратора должен предоставлять возможность контроля работоспособности Системы. |  |  |
| 2.5.2. | Интерфейс администратора должен предоставлять возможность отображения статистики работы Агентов, серверных подсистем, службы блокировки почты, СУБД, операционной системы с возможностью резервного копирования статистических данных. |  |  |
| 2.5.3. | Интерфейс администратора должен обеспечивать возможность управления службами подсистем. |  |  |
| 2.5.4. | Интерфейс администратора должен предоставлять возможность управления базами данных модулей контроля информации. |  |  |
| 2.5.5. | Интерфейс администратора должен предоставлять возможность мониторинга дискового пространства на серверах Системы. |  |  |
| 2.5.6. | Интерфейс администратора должен предоставлять возможность автоматического оповещения о важных событиях (сбои в работе, нехватка свободного места, превышение количества лицензий и другие). |  |  |
| 2.5.7. | Интерфейс администратора должен обеспечивать возможность синхронизации с одним или более доменом Active Directory. |  |  |
| 2.5.8. | Интерфейс администратора должен обеспечивать возможность работы с пользователями рабочих групп. |  |  |
| 2.5.9. | Интерфейс администратора должен предоставлять возможность разграничения прав доступа сотрудников службы безопасности к функционалу консолей подсистем и к данным по тем или иным пользователям, группам пользователей, и источникам данных. Под данными подразумеваются зафиксированные подсистемой принятия решений инциденты, а также доступное к просмотру в подсистеме контентного анализа содержимое документов и почтовых сообщений, попавших в карантин. |  |  |
| 2.5.10. | Интерфейс администратора должен обеспечивать возможность управления настройками функций сбора статистики и предоставления отчетов, а также обеспечивать возможность настройки просмотра отчетов посредством веб-интерфейса. |  |  |
| 2.5.11. | Интерфейс администратора должен предоставлять возможность автоматического переноса «старых» баз данных, индексов, хранилищ на новое место хранения (с целью разгрузки быстрых дисков), а также осуществление автоматического архивирования баз данных, индексов, хранилищ с последующей возможностью их восстановления. |  |  |
| **2.6.** | **Требования к хранению данных** |  |  |
| 2.6.1. | Для эффективной работы с большими массивами данных Система, когда это технически возможно, должна хранить оригиналы теневых копий файлов в специальном файловом хранилище, адаптированном и оптимизированном для работы с Системой. |  |  |
| 2.6.2. | Система должна иметь опцию хранения текстовой и атрибутивной информации в специализированных табличных пространствах и индексатор для выполнения полнотекстового поиска в системе. Система должна позволять выполнять поиск событий напрямую из СУБД без ожидания построения индекса в целях минимизации времени расследования инцидента. |  |  |
| 2.6.3. | Система должна быть совместима с Microsoft SQL Server 2008 SP2, PostgreSQL 13, Oracle 16 и выше для хранения информации в структурированной табличной форме и дальнейшей ее обработки в сторонних системах анализа. |  |  |
| 2.6.4. | Система должна архивировать все перехваченные объекты, а не только те, по которым зафиксированы инциденты. |  |  |
|  |  |  |  |
| **2.7.** | **Требования к надежности** |  |  |
| 2.7.1. | Должен быть предусмотрен типовой регламент действий по восстановлению работоспособности в случае отказов Системы. Процедуры восстановления работоспособности Системы должны быть описаны и задокументированы в соответствующей эксплуатационной документации на Систему. |  |  |
| 2.7.2. | Система должна быть реализована таким образом и/или определен комплекс мер и мероприятий, обеспечивающих восстановление ее работоспособности и данных при сбоях силами штатного обслуживающего персонала. |  |  |
| 2.7.3. | В случае возникновения сбоя технического или программного обеспечения Системы должна быть обеспечена возможность восстановления ее данных и настроек. |  |  |
| **3.** | **Требования к функциям (задачам), выполняемым Системой** |  |  |
| **3.1.** | **Требования к подсистеме контентного анализа** |  |  |
| 3.1.1. | Подсистема контентного анализа должна быть ориентирована на работу с данными, получаемыми от модулей подсистемы контроля. |  |  |
| 3.1.2. | Подсистема должна предоставлять возможность создания политик блокировки (помещения в карантин) трафика электронной почты, передаваемого по протоколу SMTP, а также исходящей почты, передаваемой посредством клиента Outlook по протоколам IMAP и MAPI, до принятия вердикта ответственным лицом. |  |  |
| 3.1.3. | Подсистема должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных или запротоколированных объектов, обозначенных в разделе 4: |  |  |
| • | поиск по ключевым словам и фразам в базах перехваченных документов; |  |  |
| • | выборка перехваченных данных по дате, доменному имени пользователя, адресам и хостам электронной почты, псевдонимам в Мессенджерах, именам компьютеров, принтеров и др. атрибутам; |  |  |
| • | поиск по образцу текста, схожему по смыслу или содержанию с искомым. Данный тип поиска не должен подразумевать никаких манипуляций с настройками поискового механизма и подключения дополнительных словарей, кроме задания процента релевантности (схожести) документов; |  |  |
| • | поиск по набору слов, позволяющий находить документы, содержащие определенное количество либо процент таких слов. Набор слов может быть введен вручную, вставлен из буфера обмена либо загружен из внешнего текстового файла. При формировании каждого отдельного слова из словаря не должны использоваться логические операторы. |  |  |
| • | поиск с использованием отраслевых словарей с группировкой по тематикам |  |  |
| 3.1.4. | Анализ текстового содержимого должен производиться с учетом морфологических особенностей русского языка. При этом словоформы должны образовываться без использования логических операторов и специальных символов. |  |  |
| 3.1.5. | Подсистема должна предоставлять возможности для просмотра детальной информации по каждому перехваченному объекту, в том числе возможность просмотра записи действий на экранах пользователей во встроенном видеоплеере. |  |  |
| 3.1.6. | Подсистема должна предоставлять возможность просмотра контентного маршрута перехваченного документа. |  |  |
| 3.1.7. | Подсистема должна предоставлять возможности экспорта выборки перехваченных данных (полного списка или набора файлов с оглавлением). |  |  |
| 3.1.8. | Подсистема должна предоставлять возможность формирования и отображения «Карточки пользователя», включающей в себя: общую информацию по выбранному пользователю (с возможностью добавления дополнительных полей), используемые им учетные записи из Active Directory, его контактные данные (e-mail адреса, учетные записи IM-клиентов), а также информацию по связям текущего пользователя за указанный период времени. |  |  |
| 3.1.9. | Подсистема должна предоставлять возможность просмотра информации по активности сотрудников в режиме реального времени с возможностью фильтрации по категориям активности пользователя. |  |  |
| 3.1.10. | Подсистема должна обеспечивать возможность оперативного контроля за происходящим на рабочих местах пользователей в режиме реального времени: просмотр происходящего на экранах мониторов, прослушивание речи сотрудников, просмотр происходящего за компьютером посредством подключенной веб-камеры. |  |  |
| 3.1.11. | Подсистема должна предоставлять возможность генерации отчетов по имеющимся базовым шаблонам, а также предусматривать возможность добавления пользовательских шаблонов. |  |  |
| 3.1.12. | Подсистема должна поддерживать предоставление отчетов в табличном, диаграммном, в виде временного графика, а также в виде интерактивного графа связей с возможностью фильтрации событий по различным метрикам. |  |  |
| 3.1.13. | Подсистема должна производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности. |  |  |
| 3.1.14. | Подсистема должна отображать информацию по активности пользователей в запускаемых ими приложениях в течение рабочего дня. При нарушениях сотрудниками установленного в компании трудового распорядка (поздний приход, ранний уход, недостаточная активность; длительная работа в приложениях, не связанных с рабочей деятельностью), должна быть предусмотрена возможность формирования оповещения по данному факту с последующей отправкой его на электронный адрес сотрудника службы информационной безопасности. |  |  |
| 3.1.15. | Подсистема должна генерировать краткие и детальные отчеты по продуктивности работы пользователей за выбранный период времени. |  |  |
| 3.1.16. | Подсистема должна генерировать отчеты по устройствам: перечень установленного оборудования на компьютерах пользователей и отчет по изменениям в устройствах (комплектующих) компьютеров. |  |  |
| 3.1.17. | Подсистема должна отображать: |  |  |
| • | операции с агентами/протоколами, совершенные любым либо указанным пользователем; |  |  |
| • | список компьютеров с нерабочими агентами; |  |  |
| • | список компьютеров без агентов; |  |  |
| • | информацию о количестве сообщений по выбранным компьютерам за заданный промежуток времени. |  |  |
| 3.1.18. | Подсистема должна предоставлять возможность быстрого перехода к поиску и просмотру найденных документов. |  |  |
| 3.1.19. | Подсистема должна предоставлять возможность переходов по связанным отчетам. |  |  |
| 3.1.20. | Подсистема должна предусматривать представление связей между внутренними и внешними адресатами в виде интерактивного графа для получения наглядного представления о круге общения выбранного пользователя или нескольких пользователей, выявления общих контактов для данных пользователей, а также контактов внешних адресатов с сотрудниками компании. |  |  |
| 3.1.21. | Подсистема должна обеспечивать получение наглядного представления об адресах, с которых выбранный пользователь отправлял либо на которые получал сообщения. |  |  |
| 3.1.22. | Подсистема должна предусматривать возможность конвертации сгенерированных отчетов в PDF-файл, равно как и вывод их на печать. |  |  |
| **3.2.** | **Требования к подсистеме принятия решений** |  |  |
| 3.2.1. | Подсистема должна иметь изолированное разграничение прав доступа. |  |  |
| 3.2.2. | Подсистема должна выносить единый вердикт (инцидент / не инцидент) для каждого перехваченного объекта. |  |  |
| 3.2.3. | Подсистема должна предоставлять возможности для ведения журнала инцидентов с возможностью рубрикации по каналам передачи данных, протоколам, пользователям, правилам проверки. |  |  |
| 3.2.4. | Подсистема должна предоставлять возможность уведомления ответственных лиц об инцидентах по электронной почте. |  |  |
| 3.2.5. | Подсистема должна предоставлять возможности для задания правил автоматического вынесения вердикта по объекту (инцидент / не инцидент). Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании: |  |  |
| • | формальных признаков перехваченного объекта (доменное имя, отправитель, получатель, хост, размер, расширение файла, канал передачи данных, протокол и т.д.); |  |  |
| • | защищенных паролем архивов; |  |  |
| • | результатов контентного анализа текста, извлеченного из перехваченных объектов (по словам и образцам текстов, тематическим словарям, путем сравнения с базой эталонных документов, путем поиска текстов, близких по смыслу или содержанию с эталоном, поиска алфавитно-цифровых объектов, а также поиска с использованием регулярных выражений). |  |  |
| • | результатов анализа графических объектов (сканы паспортов, кредиток, схем, чертежей и т.д.) без использования технологии OCR |  |  |
| • | результатов анализа информации содержащейся в эталонной выгрузке БД с возможностью создания логических условий поиска по комбинациям строк и столбцов |  |  |
| • | результатов анализа документов с печатями различных подразделений |  |  |
| 3.2.6. | Подсистема должна предоставлять возможности для изменения существующих и применения новых правил автоматического вынесения вердикта (правил проверки). |  |  |
| 3.2.7. | Подсистема должна предоставлять возможность выполнения ретроспективного контроля перехваченных документов. |  |  |
| 3.2.8. | Подсистема должна предусматривать возможность объединения политик безопасности (правил проверки) в группы. |  |  |
| 3.2.9. | Подсистема должна предоставлять возможность задания для каждой группы политик безопасности индивидуальных настроек: перечня источников данных, по которым будет проводиться опрос, расписания проверки, списка получателей оповещений об инцидентах, списка исключений. |  |  |
| 3.2.10. | Подсистема должна предоставлять возможность экспорта/импорта структуры настроек. |  |  |
| 3.2.11. | Подсистема должна предоставлять возможность добавления пользователей и наделения их правами просмотра и редактирования тех или иных политик безопасности и списков исключений, в том числе возможность выставления запрета на данные действия. |  |  |
| 3.2.12. | Подсистема должна предоставлять возможности протоколирования выявленных инцидентов. |  |  |
| 3.2.13. | Подсистема должна поддерживать возможность категоризации инцидентов с помощью цветовых меток. |  |  |
| 3.2.14. | Подсистема должна поддержать возможность экспорта данных об инцидентах и событиях посредством syslog. |  |  |
| 3.2.15. | Подсистема должна предоставлять возможность подбора паролей для перехваченных архивов, защищенных паролем. База (словарь) для перебора паролей генерируется автоматически на базе данных модуля контроля данных, вводимых с клавиатуры. |  |  |
| 3.2.16. | Подсистема должна предоставлять возможности для принятия решений в отношении следующих типов объектов: |  |  |
| • | сообщений, переданных по поддерживаемым Системой каналам и протоколам; |  |  |
| • | файлов форматов: MS Office (doc, docx, dot, xls, xlsx, xlsb, xlsm, xlt, xltx, xltm, ppt, pptx, rtf, pot, vsd, vst, vsdx), Open Office (sxw, stw, odt, ods), HTML-файлы (htm, html, shtml, mht, css, js, maff), файлы почтовых сообщений (eml, msg), базы данных (mdb), дополнительные форматы документов (txt, xml, pdf, djvu, csv, lst, log, bat, ini, wri); |  |  |
| • | распознанных и проанализированных текстов в графических файлах форматов bmp, jpg, jpeg, png, tif, tiff, gif; |  |  |
| • | документов, вложенных в сжатые файлы: rar, zip, 7z, jar, tar, arj, gz, gzip, cab, iso, chm, hlp, 001. |  |  |
| 3.2.17. | Подсистема должна обеспечить наличие следующих возможностей обнаружения критичной информации: |  |  |
| • | по ключевым словам, в том числе с возможностью ограничений по взаимному расположению искомых слов и с учетом морфологических особенностей и синонимии русского языка; |  |  |
| • | возможность обнаружения похожих документов на основе образца, схожего по содержанию с искомым; |  |  |
| • | по формальным признакам сообщений и файлов (доменный пользователь, имя компьютера, отправитель, получатель, размер, имя файла, формат и др.), в том числе для файлов, из которых не может быть извлечен текст; |  |  |
| • | по заранее заданному словарю с целью выявления определенных типов документов (резюме, финансовые и бухгалтерские отчеты); |  |  |
| • | возможность создания комплексных поисковых запросов, включающих в себя несколько критериев (фразовый поиск, поиск по абзацам и целым документам и атрибутам), объединенных логическими операторами AND, OR, NOT; |  |  |
| • | по регулярным выражениям PCRE – поиск сложных алфавитно-цифровых объектов (номера паспортов, индивидуальные номера налогоплательщиков, номера кредитных карт, договоров или счетов, кодов классификаторов и т.п.), с возможностью создания комплексных регулярных выражений (состоящих из нескольких простых), задания порога срабатывания по суммарному количеству регулярных выражений, количеству вхождений регулярного выражения в документ и количеству промежуточных символов между регулярными выражениями, возможностью использования как стандартных выражений, включенных в дистрибутив, так и создание пользовательских, а также с возможностью проверки полученных результатов; |  |  |
| • | по цифровым отпечаткам конфиденциальных документов, с возможностью указания порога срабатывания; |  |  |
| • | по значениям атрибутов (как общих атрибутов, так и уникальных для отдельных каналов связи); |  |  |
| 3.2.18. | Подсистема должна предусматривать наличие нескольких встроенных словарей. |  |  |
| 3.2.19. | Подсистема должна обеспечивать устойчивость к следующим видам манипуляции с информацией: |  |  |
| • | импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными; |  |  |
| • | изменение порядка слов; |  |  |
| • | изменения расстояний между словами; |  |  |
| • | изменение форматирования документа; |  |  |
| • | изменение словоформ; |  |  |
| • | замены букв на символы другого алфавита; |  |  |
| • | использование цифр вместо букв; |  |  |
| • | изменение расширений файлов. |  |  |
| 3.2.20. | Подсистема должна предоставлять возможности для просмотра детальной информации по каждому инциденту. |  |  |
| **4.** | **Требования к подсистеме контроля** |  |  |
| **4.1.** | **Общие требования к функциям Агента для ОС Windows** |  |  |
| **4.1.1.** | **Требования к модулю контроля электронной почты** |  |  |
| 4.1.1.1. | Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, MAPI, HTTP (веб-почта: как исходящая, так и входящая), при помощи почтовых клиентов или браузеров. Модуль должен иметь подключаемую функцию автоматической остановки исходящих почтовых сообщений по протоколам SMTP и HTTP, а также блокировки исходящих электронных сообщений, передаваемых с помощью почтового клиента Outlook по протоколам IMAP и MAPI, на основе контентного и/или контекстного анализа как почтовых сообщений, так и вложений. |  |  |
| 4.1.1.2. | Модуль должен предоставлять возможность блокировки исходящей почты по контентным и/или контекстным критериям на почтовом сервере с возможностью работы в разрыв. |  |  |
| 4.1.1.3. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др. |  |  |
| **4.1.2.** | **Требования к модулю контроля сервисов обмена мгновенными сообщениями** |  |  |
| 4.1.2.1. | Модуль должен обеспечивать контроль: |  |  |
| • | входящих/исходящих сообщений и файлов, переданных пользователями по протоколам: |  |  |
| - | OSCAR (ICQ/QIP), |  |  |
| - | XMPP (Cisco Jabber), |  |  |
| - | MMP (Агент Mail.ru); |  |  |
| • | входящих и исходящих сообщений по протоколу HTTP в социальных сетях: |  |  |
| - | Facebook, |  |  |
| - | LinkedIn, |  |  |
| - | ВКонтакте, |  |  |
| - | Moй Мир@Mail.ru, |  |  |
| - | Одноклассники.ru, |  |  |
| • | чатов, файлов, переданных при помощи desktop-версий мессенджеров: |  |  |
| - | Skype, |  |  |
| - | Lync, |  |  |
| - | Viber, |  |  |
| - | Telegram, |  |  |
| - | WhatsApp, |  |  |
| - | Rocket.chat, |  |  |
| • | чатов, файлов веб-версий мессенджеров: |  |  |
| - | Skype (web.skype.com), |  |  |
| - | Telegram (web.telegram.org), |  |  |
| • | чатов, звонков и файлов, переданных при помощи: |  |  |
| - | Zoom Chat, |  |  |
| - | TrueConf Client, |  |  |
| - | конференций Zoom; |  |  |
| • | сообщений и файлов ресурса slack.com. |  |  |
| 4.1.2.2. | Модуль должен осуществлять контроль сеансов текстовой и голосовой связи, файлов при помощи Skype. |  |  |
| 4.1.2.3. | Модуль должен обеспечивать контроль входящих/исходящих сообщений, файлов коммуникационных программ-клиентов Microsoft Lync, Viber и Telegram. |  |  |
| 4.1.2.4. | Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования. |  |  |
| 4.1.2.5. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др. |  |  |
|  |  |  |  |
| **4.1.3.** | **Требования к модулю контроля FTP-соединений** |  |  |
| 4.1.3.1. | Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединения, в том числе с применением SSL-шифрования. |  |  |
| 4.1.3.2. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др. |  |  |
| 4.1.3.3. | Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище. |  |  |
| **4.1.4.** | **Требования к модулю контроля HTTP-трафика** |  |  |
| 4.1.4.1. | Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов). |  |  |
| 4.1.4.2. | Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome; Edge. |  |  |
| 4.1.4.3. | Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo. |  |  |
| 4.1.4.4. | Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB). |  |  |
| 4.1.4.5. | Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение. |  |  |
| 4.1.4.6. | Модуль должен обеспечивать вычитку сохраненных в браузерах авторизационных данных пользователей к интернет-ресурсам, а также позволять осуществление подбора мастер-пароля в случаях, если данные защищены. |  |  |
| 4.1.4.7. | Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков, а также использование категорий сайтов для блокировки и/или разрешения посещения интернет-ресурсов, предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу. |  |  |
| 4.1.4.8. | Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту. |  |  |
| 4.1.4.9. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др. |  |  |
| **4.1.5.** | **Требования к модулю контроля печати** |  |  |
| 4.1.5.1. | Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров. |  |  |
| 4.1.5.2. | Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов. |  |  |
| 4.1.5.3. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др. |  |  |
| **4.1.6.** | **Требования к модулю контроля съёмных устройств** |  |  |
| 4.1.6.1. | Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (СD-/DVD-приводы, съемные накопители USB и FireWire, USB-устройства, Wi-Fi и Bluetooth) и портам (USB, FireWire, COM, LPT, IRDA + IDE/SATA, Serial Port, Parallel Port, PCI, SCSI и прочее). |  |  |
| 4.1.6.2. | Модуль должен поддерживать работу в терминальной сессии. |  |  |
| 4.1.6.3. | Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов. |  |  |
| 4.1.6.4. | Модуль должен предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство. |  |  |
| 4.1.6.5. | Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве. |  |  |
| 4.1.6.6. | Модуль должен предоставлять возможность теневого копирования данных, передаваемых через буфер обмена, в том числе буфер обмена RDP-сессии. |  |  |
| 4.1.6.7. | Модуль должен предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе. |  |  |
| 4.1.6.8. | Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение». |  |  |
| 4.1.6.9. | Модуль должен предоставлять возможность блокировки записи на подключаемые внешние USB-устройства, исходя из формальных признаков файлов (имя файла, формат), а также по содержимому передаваемых данных. |  |  |
| 4.1.6.10. | Модуль должен предоставлять возможность запрета копирования данных, передаваемых через RDP-сессию. |  |  |
| 4.1.6.11. | Модуль должен позволять ограничение установки RDP-подключения как на удаленные рабочие станции или серверы, так и на рабочую станцию или сервер с работающим модулем. |  |  |
| 4.1.6.12. | Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя. |  |  |
| 4.1.6.13. | Модуль должен предоставлять возможность блокировки Bluetooth-устройств и сервисов. |  |  |
| 4.1.6.14. | Модуль должен предоставлять возможность контроля буфера обмена на компьютере пользователя, а также блокировку передачи данных через буфер обмена по содержимому копируемых данных. |  |  |
| 4.1.6.15. | Модуль должен предоставлять возможность использования «белых списков» устройств, к которым в дальнейшем пользователь будет иметь неограниченный доступ либо доступ «только чтение», а также «черных списков» устройств, доступ к которым будет заблокирован. |  |  |
| 4.1.6.16. | Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др. |  |  |
| **4.1.7.** | **Требования к модулю контроля событий на мониторах и действий сотрудников** |  |  |
| 4.1.7.1. | Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции и/или при вводе пользователем ключевых слов. |  |  |
| 4.1.7.2. | Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, звонке |  |  |
| 4.1.7.3. | Модуль должен обеспечивать видеозапись происходящего на экранах мониторов согласно настроенному расписанию или событиям, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции и/или при вводе пользователем ключевых слов. |  |  |
| 4.1.7.4. | Модуль должен обеспечивать создание снимков, видеозаписи посредством подключенной к рабочей станции веб-камеры по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции, с возможностью использования нескольких веб-камер. |  |  |
| 4.1.7.5. | Модуль должен позволять скорректировать расписание создания снимков при посещении определенных (настроенных заранее) интернет-узлов, авторизации в операционной системе, отсутствии пользовательских сессий. |  |  |
| 4.1.7.6. | Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи. |  |  |
| 4.1.7.7. | Модуль должен обеспечивать одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени. |  |  |
| 4.1.7.8. | Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры в режиме реального времени. |  |  |
| 4.1.7.9. | Модуль должен предоставлять возможность экспорта перехваченных снимков экрана и видеозаписей в отдельную папку. |  |  |
| 4.1.7.10. | Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний. |  |  |
| 4.1.7.11. | Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена. |  |  |
| 4.1.7.12. | Модуль должен обеспечивать возможность блокировки нажатий клавиши «PrintScreen». |  |  |
| 4.1.7.13. | Модуль должен выделять и позволять исключать из аудита набранные символы, если они являются вводом пароля для всех случаев, когда это технически возможно. |  |  |
| 4.1.7.14. | Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов. |  |  |
| 4.1.7.15. | Модуль должен предоставлять возможность поиска, вводимого с клавиатуры или помещаемого в буфер обмена содержимого за определенный период времени применительно к заданным пользователям, компьютерам, именам запущенных процессов, MAC- и IP-адресам, продолжительности работы в приложении. |  |  |
| **4.1.8.** | **Требования к модулю контроля разговоров сотрудников** |  |  |
| 4.1.8.1. | Модуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.), а также иметь возможность аудиозаписи с выхода звуковой карты. |  |  |
| 4.1.8.2. | Модуль должен предусматривать возможность активации записи голосов по расписанию, при запуске определенных процессов, внутри офиса/за его пределами (в командировке), при отсутствии авторизованных пользователей в операционной системе, автоматической активации микрофона при деактивации его пользователями в настройках ОС, а также возможность настройки качества записываемого звукового файла. |  |  |
| 4.1.8.3. | Модуль должен обеспечивать помещение записанных звуковых файлов в базу данных либо использовать для хранения бинарных данных файловое хранилище. |  |  |
| 4.1.8.4. | Модуль должен предоставлять возможность экспорта перехваченных разговоров в отдельную папку. |  |  |
| **4.1.9.** | **Требования к модулю контроля активности пользователей и приложений** |  |  |
| 4.1.9.1. | Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах. |  |  |
| 4.1.9.2. | Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером. |  |  |
| 4.1.9.3. | Модуль должен иметь подключаемую возможность автоматической категоризации любых посещенных сайтов на тематические группы, используя заранее загруженную и регулярно пополняемую базу классификации сайтов. |  |  |
| **4.1.10.** | **Требования к модулю контроля облачных хранилищ данных** |  |  |
| 4.1.10.1. | Модуль должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов: |  |  |
| • | Google Drive, |  |  |
| • | OneDrive, |  |  |
| • | Office 365, |  |  |
| • | DropBox, |  |  |
| • | Evernote, |  |  |
| • | Яндекс.Диск, |  |  |
| • | iCloud, |  |  |
| • | DropMeFiles, |  |  |
| • | OwnCloud, |  |  |
| • | SharePoint, |  |  |
| 4.1.10.2. | Модуль должен обеспечивать контроль файлов, передаваемых в программах удаленного доступа: |  |  |
| • | TeamViewer, |  |  |
| • | AnyDesk |  |  |
| 4.1.10.3. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др. |  |  |
| 4.1.10.4. | Модуль должен обеспечивать возможность блокировки передачи в облачные хранилища посредством веб-браузера файлов, соответствующих определенному контенту и/или контексту, за исключением трафика вне спецификации HTTPS. |  |  |
| **4.2.** | **Общие требования к функциям Агента для ОС Linux** |  |  |
| **4.2.1.** | **Требования к модулю контроля электронной почты** |  |  |
| 4.2.1.1. | Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, HTTP (веб-почта: как исходящая, так и входящая) при помощи любых почтовых клиентов или браузеров. Иметь подключаемую функцию автоматической остановки исходящих почтовых сообщений по протоколам SMTP, на основе контентного и/или контекстного анализа как почтовых сообщений, так и вложений. |  |  |
| 4.2.1.2. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др. |  |  |
| **4.2.2.** | **Требования к модулю контроля сервисов обмена мгновенными сообщениями** |  |  |
| 4.2.2.1. | Модуль должен обеспечивать контроль: |  |  |
| • | входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), XMPP (Jabber, Google Hangouts), MMP (Агент Mail.ru), SIP (X-Lite и др.) и др.; |  |  |
| • | входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Moй Мир@Mail.ru, Одноклассники.ru, Google+, Мамба.ru и прочее); |  |  |
| 4.2.2.2. | Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования. |  |  |
| 4.2.2.3. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др. |  |  |
| **4.2.3.** | **Требования к модулю контроля FTP-соединений** |  |  |
| 4.2.3.1. | Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединение, в том числе с применением SSL-шифрования. |  |  |
| 4.2.3.2. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др. |  |  |
| **4.2.4.** | **Требования к модулю контроля HTTP-трафика** |  |  |
| 4.2.4.1. | Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов). |  |  |
| 4.2.4.2. | Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Mozilla Firefox; Opera; Google Chrome. |  |  |
| 4.2.4.3. | Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo. |  |  |
| 4.2.4.4. | Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB). |  |  |
| 4.2.4.5. | Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение. |  |  |
| 4.2.4.6. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др. |  |  |
| **4.2.5.** | **Требования к модулю контроля печати** |  |  |
| 4.2.5.1. | Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров. |  |  |
| 4.2.5.2. | Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов. |  |  |
| 4.2.5.3. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др. |  |  |
| 4.2.5.4. | Модуль должен поддерживать возможность исключения из контроля отдельных принтеров (в том числе по их описанию и месту расположения), пользователей. |  |  |
| **4.2.6.** | **Требования к модулю контроля и управления доступом съёмных устройств** |  |  |
| 4.2.6.1. | Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (съемные накопители USB, Wi-Fi и сетевым папкам, модемам и сетевым адаптерам). |  |  |
| 4.2.6.2. | Модуль должен поддерживать работу в терминальной сессии. |  |  |
| 4.2.6.3. | Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов. |  |  |
| 4.2.6.4. | Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве или записываемых на внешнее USB-устройство. |  |  |
| 4.2.6.5. | Модуль должен предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство через буфер обмена, в том числе буфер обмена RDP-сессии. |  |  |
| 4.2.6.6. | Модуль должен предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе. |  |  |
| 4.2.6.7. | Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение». |  |  |
| 4.2.6.8. | Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др. |  |  |
| **4.2.7.** | **Требования к модулю контроля событий на мониторах и действий сотрудников** |  |  |
| 4.2.7.1. | Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции. |  |  |
| 4.2.7.2. | Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи. |  |  |
| 4.2.7.3. | Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний. |  |  |
| 4.2.7.4. | Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена. |  |  |
| 4.2.7.5. | Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов. |  |  |
| **4.2.8.** | **Требования к модулю контроля разговоров сотрудников** |  |  |
| 4.2.8.1. | Модуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.). |  |  |
| 4.2.8.2. | Модуль должен предусматривать возможность активации записи голосов по расписанию, внутри офиса/за его пределами (в командировке), а также возможность настройки качества записываемого звукового файла. |  |  |
| **4.2.9.** | **Требования к модулю контроля активности пользователей и приложений** |  |  |
| 4.2.9.1. | Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях. |  |  |
| 4.2.9.2. | Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером. |  |  |
|  |  |  |  |
| 4.2.10. | Требования к модулю контроля облачных хранилищ данных |  |  |
| 4.2.10.1. | Модуль должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов Google Drive, Google Docs, OneDrive, SkyDrive, Office 365, DropBox, Evernote, Яндекс.Диск, Cloud.mail.ru, Amazon S3, iCloud, DropMeFiles, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia, My-Files, Nextcloud, Seafile, SharePoint, Acronis File Advanced, Cloudian S3 storage, Disk Bitrix24. |  |  |
| 4.2.10.2. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др. |  |  |
| **4.3.** | **Общие требования к функциям Агента для ОС MacOS** |  |  |
| **4.3.1.** | **Требования к модулю контроля событий на мониторах и действий сотрудников** |  |  |
| 4.3.1.1. | Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции. |  |  |
| 4.3.1.2. | Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи. |  |  |
| 4.3.1.3. | Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний. |  |  |
| 4.3.1.4. | Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена. |  |  |
| 4.3.1.5. | Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов. |  |  |
| **4.3.2.** | **Требования к модулю контроля активности пользователей и приложений** |  |  |
| 4.3.2.1. | Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях. |  |  |
| 4.3.2.2. | Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером. |  |  |
| **4.4.** | **Требования к функциям контроля данных на уровне сетевого перехвата (при интеграции с прокси-сервером (по протоколу ICAP) либо сетевым оборудованием через зеркалирование трафика (SPAN))** |  |  |
| **4.4.1.** | **Требования к модулю контроля электронной почты** |  |  |
| 4.4.1.1. | Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, HTTP (веб-почта: как исходящая, так и входящая), при помощи почтовых клиентов или браузеров. При этом нешифрованный трафик HTTP доступен в как в режиме зеркалирования, так и в режиме интеграции с прокси-сервером. Нешифрованный SMTP, POP3 и IMAP трафик доступен только в режиме зеркалирования. Шифрованный HTTP(S) трафик доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата. |  |  |
| 4.4.1.2. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др. |  |  |
| **4.4.2.** | **Требования к модулю контроля сервисов обмена мгновенными сообщениями** |  |  |
| 4.4.2.1. | Модуль должен обеспечивать контроль в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата: |  |  |
| • | входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Moй Мир@Mail.ru, Одноклассники.ru, Google+, Мамба.ru и других, на усмотрение Разработчика Системы); |  |  |
| • | чатов, файлов веб-версии Skype (web.skype.com); |  |  |
| • | чатов, файлов веб-версий мессенджеров: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost; |  |  |
| • | истории передачи файлов и чатов Instagram, VK Teams; |  |  |
| • | сообщений и файлов ресурса slack.com. |  |  |
| 4.4.2.2. | Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, передаваемых по протоколу HTTP в социальных сетях и веб-мессенджерами (Rocket.chat, Mattermost и др.), соответствующих определенному контексту. |  |  |
| 4.4.2.3. | Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования. |  |  |
| 4.4.2.4. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др. |  |  |
| **4.4.3.** | **Требования к модулю контроля FTP-соединений** |  |  |
| 4.4.3.1. | Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединения, в том числе с применением SSL-шифрования в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата |  |  |
| 4.4.3.2. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др. |  |  |
| 4.4.3.3. | Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище. |  |  |
| **4.4.4.** | **Требования к модулю контроля HTTP-трафика** |  |  |
| 4.4.4.1. | Контроль защищенного HTTPS трафика может быть доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата. |  |  |
| 4.4.4.2. | Контроль незащищенного HTTP трафика может быть доступен как режиме интеграции с прокси-сервером, так и в режиме зеркалирования трафика. |  |  |
| 4.4.4.3. | Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов). |  |  |
| 4.4.4.4. | Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome. |  |  |
| 4.4.4.5. | Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB). |  |  |
| 4.4.4.6. | Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение. |  |  |
| 4.4.4.7. | Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков, а также использование категорий сайтов для блокировки и/или разрешения посещения интернет-ресурсов, предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу. |  |  |
| 4.4.4.8. | Модуль должен обеспечивать возможность блокировки передачи запросов, соответствующих определенному контексту. |  |  |
| 4.4.4.9. | Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др. |  |  |

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ФИО

**Приложение 3 к Приглашению**

**Проект ДОГОВОРА**

**о поставке программного обеспечения**

г. Бишкек «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** в дальнейшем именуемое «**Сторона-1**», в лице директора \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании Устава, с одной стороны, и

**ЗАО «Альфа Телеком»**, именуемое в дальнейшем **«Сторона-2»**, в лице Генерального директора Мамытова Н.Т., действующего на основании Устава, с другой стороны, и совместно именуемые Стороны, заключили настоящий Договор о нижеследующем.

**1. Предмет договора**

* 1. Сторона-1 обязуется осуществить поставку Стороне-2 программного обеспечения и лицензионных ключей (далее – ПО) и доступ к технической поддержке на условиях постоянной неисключительной лицензии на его использование в количестве, по ценам и техническим параметрам, указанным в Приложении 1 к настоящему Договору (далее Спецификация), являющихся неотъемлемой частью настоящего Договора, а Сторона-2, в свою очередь, принимает надлежаще поставленное ПО/права и осуществляет оплату в порядке и размере, предусмотренном разделом 3 настоящего Договора.
  2. Все приложения и дополнительные соглашения к настоящему Договору являются неотъемлемой его частью.

**2. Права и обязанности сторон**

**2.1. Обязанности Стороны-1**

* + 1. Передать Стороне-2 по Акту приема-передачи ПО и право пользования технической поддержкой, которое включает в себя: лицензии, возможность получения новых версий ПО, обновлений, технической помощи по установке, настройке, устранению проблем в работе ПО, в строгом соответствии со Спецификацией к настоящему Договору, в порядке и на условиях, предусмотренных настоящим Договором и в строгом соответствии с Приложением 1.
    2. Незамедлительно информировать Сторону-2 о невозможности исполнения обязательств, в срок, предусмотренный настоящим Договором.
    3. Известить Сторону-2 по эл. почте [InfSecurity@megacom.kg](mailto:InfSecurity@megacom.kg) о предоставления права пользования ПО и технической поддержкой, а также способ получения доступа к установочным файлам ПО, инструкциям.
    4. Оповестить Сторону-2 об изменении юридического/фактического адреса, либо банковских реквизитов в течение 3 (трех) рабочих дней со дня их изменения.
    5. Сторона-1 гарантирует, что действует в рамках полномочий и объема прав, предоставленных ему правообладателем исключительных имущественных авторских прав на ПО.
    6. Сторона-1 подтверждает, что в случае превышения предоставления объема прав, предоставленных ему Правообладателем ПО, Сторона-1 несет ответственность перед Правообладателем ПО самостоятельно. В случае если такое превышение полномочий впоследствии сделает невозможным использование технической поддержки Стороной-2, то Сторона-1 обязуется возвратить денежные средства, полученные по настоящему Договору от Стороны-2.
  1. **Обязанности Стороны-2:**
     1. Принять от Стороны-1 надлежаще переданное ПО и право пользования технической поддержкой и произвести оплату в соответствии с условиями настоящего Договора, в частности, с разделом 3 настоящего Договора.
     2. Оповестить Сторону-1 об изменении юридического/фактического адреса, электронного адреса, либо банковских реквизитов в течение 3 (трех) рабочих дней со дня их изменения.
     3. Передавать Стороне-1 необходимую информацию для выполнения обязательств по настоящему Договору.

**2.3. Права Стороны-2:**

**2.3.1.** В случае не предоставления Стороной-1 Стороне-2 прав доступа к ПО и технической поддержкой или несвоевременного предоставления таких прав согласно Договора, Сторона-2 вправе взыскать со Стороны-1 причиненные убытки и/или расторгнуть настоящий договор в одностороннем порядке.

**3. Стоимость договора и порядок оплаты**

* 1. Общая стоимость настоящего Договора составляет: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**сомов, с учетом всех налогов, предусмотренных действующим законодательством Кыргызской Республики для данных правоотношений. НДС 12% составляет **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сом, НсП=0%. Сторона-1 – плательщик НДС.

Стоимость Договора является окончательной и изменению не подлежит.

* 1. Сторона-2 осуществляет оплату по настоящему Договору в следующем порядке:

100 % от общей стоимости Договора, в течение 10 банковских дней с момента получения Стороной-2 оригинала счета-фактуры, выставленного Стороной-1 на основании подписанного сторонами и датой Акта приема-передачи прав доступа к ПО и технической поддержке.

* 1. Если Сторона-1 – плательщик НДС в период действия Договора меняет свой налоговый статус в отношении НДС, она обязана известить об этом Сторону-2 в течение 3 (трех) рабочих дней. При этом стоимость Договора подлежит пересчету на сумму обозначенного ранее НДС по п. 3.1. Если по какой-либо причине Сторона-1 не сможет выставить и предоставить счет-фактуру по НДС Стороне-2 по предоставлении прав доступа к технической поддержке, Стороны соглашаются с тем, что стоимость Договора подлежит пересчету на сумму обозначенного ранее НДС по п.3.1.
  2. При возникновении обстоятельств, указанных в п.3.3 Сторона-2 оплачивает сумму, указанную в 3.1., за вычетом суммы НДС в размере: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сом безакцептно, т.е. оплате подлежит сумма **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**.
  3. Если по любым причинам в дальнейшем счет-фактура Стороны-1 будет признан недействительным/утерянным/испорченным, Сторона-1 обязан известить об этом Сторону-2 и вернуть Стороне-2 сумму НДС по такому счету-фактуре в течение 10 рабочих дней.
  4. Оплата по настоящему договору осуществляется Стороной-2 в сомах путем перечисления денежных средств на расчетный счет Стороны-1, указанный в п.13 Договора.

**4. Порядок передачи прав**

**4.1.** Сторона-1 обязана передать Стороне-2 право доступа к ПО и технической поддержкой путем предоставления официального письма производителя (правообладателя исключительных прав ПО), о чем уведомляет Сторону-2 по эл. почте[InfSecurity@megacom.kg](mailto:InfSecurity@megacom.kg) в течении 10 (десяти) рабочих дней с момента заключения договора. Срок действия прав доступа к технической поддержке определяется в Приложении 1 к Договору.

**4.2.** Не позднее истечения двух рабочих дней, следующих за днем получения извещения, Сторона-2 осуществляет проверку полученных прав доступа к ПО и лицензионных ключей на соответствие Спецификации. При соответствии переданных прав Спецификации Сторона-2 подписывает Акт приема-передачи прав доступа к ПО и технической поддержке, и возвращает один экземпляр Акта Стороне-1. В случае если переданные права не соответствуют Приложению 1 к Договору, тогда Сторона-2 в этот же срок направляет мотивированный отказ от приемки или Стороны составляют Акт о выявленных несоответствиях, в котором Стороны согласовывают между собой срок устранения несоответствий, (но не более чем 10 рабочих дней) в течение которого Сторона-1 обязана устранить выявленные несоответствия. Установление срока устранения несоответствий не исключает наступления ответственности за нарушение Стороной-1 срока предоставления прав доступа к ПО и технической поддержке согласно пункту 6.2.

**4.3.** Факт передачи прав доступа к ПО, лицензиям и технической поддержке Стороной-2 подтверждается Актом приема-передачи прав доступа согласно Приложения 2 к Договору. С момента подписания Сторонами Акта обязанность Стороны-1 по передаче соответствующих прав считается исполненной.

**5. Гарантийное обеспечение исполнения договора**

**5.1.** Гарантийное обеспечение исполнения Договора Сторона-1 вносит в течение 5 банковских дней с момента заключения настоящего Договора в размере **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ сом**, составляющее **\_\_**% от общей суммы Договора. Гарантийное обеспечение исполнения Договора остается у Стороны-2 до подписания Акта приема-передачи прав доступа к ПО и технической поддержке.

**5.2.** В случае ненадлежащего исполнения или неисполнения Стороной-1 принятых на себя обязательств по настоящему Договору, Сторона-2 вправе, после направления требования об уплате неустойки Стороне-1 согласно условиям Договора, а именно п.6.5., в безакцептном порядке удержать из гарантийного обеспечения исполнения договора начисленную неустойку, а также убытки, которые могут наступить вследствие неполного/ненадлежащего исполнения или неисполнения Стороной-1 своих обязательств по настоящему Договору и/или в случае недостаточности суммы гарантийного обеспечения исполнения договора – удержать после направления требования об уплате неустойки, Стороне-1 согласно условиям Договора, а именно п.6.5., всю сумму гарантийного обеспечения исполнения договора и недостающую сумму из суммы оплаты.

**5.3.** Сторона-2 возвращает Стороне-1 сумму гарантийного обеспечения исполнения Договора в случае надлежащего исполнения Стороной-1 своих обязательств в течение 10 (десяти) рабочих дней с момента подписания Акта, подтверждающего предоставление права пользования ПО и технической поддержкой.

**5.4.** В целях обеспечения надлежащего исполнения договорных обязательств на период срока технической поддержки, Сторона-2 сохраняет у себя часть суммы ГОИД - в размере 10 % от суммы ГОИД, указанной в п. 5.1. Договора.

* 1. Оставшаяся сумма гарантийного обеспечения исполнения договора, после удержания из ГОИД неустоек согласно п. 6.3 Договора и сохранения части ГОИД согласно п. 5.4. Договора, возвращается Стороне-1 в течение 10-ти (десять) банковских дней со дня подписания Акта приема – передачи оказанных услуг.
  2. После выполнения Стороной-1 договорных обязательств по договору, Сторона-2 возвращает Стороне-1 оставшуюся сумму ГОИД, в течение десяти рабочих дней.
  3. В случае не внесения Стороной-1 ГОИД в срок, установленный в п. 5.1 Договора, Сторона-2 вправе расторгнуть Договор в порядке, предусмотренном в п. 10.1 Договора.

**6. Ответственность сторон**

**6.1.** За неисполнение или ненадлежащее исполнение обязательств по настоящему Договору стороны несут ответственность в соответствии с условиями настоящего Договора, а в случаях, не предусмотренных Договором, в соответствии с действующим законодательством Кыргызской Республики.

**6.2**. В случае нарушения Стороной-1 срока предоставления прав доступа к ПО и технической поддержке, указанного в п. 4.1. Договора, а также нарушения Стороной-1 сроков устранения несоответствий согласно п.4.2. Договора, Сторона-2 удерживает в безакцепном порядке из суммы, подлежащей оплате и/или из суммы гарантийного обеспечения исполнения договора неустойку в размере 0,1 (ноль целых одна десятая) % от суммы настоящего Договора за каждый день просрочки передачи прав, но не более 5 (пяти) % от общей стоимости Договора.

**6.3.** В случае если Сторона-1 передала Стороне-2 права не соответствующие Спецификации, Сторона-2 удерживает в безакцепном порядке из суммы, подлежащей оплате и/или из суммы гарантийного обеспечения исполнения договора неустойку в размере 0.1 (ноль целых одна десятая) % от стоимости Договора, за каждый день просрочки, с должной даты передачи прав до даты фактической передачи, но не более 5 (пяти) % от общей стоимости Договора.

**6.4.** В случае нарушения Стороной-2 сроков оплаты, указанных в п. 3.2. Договора, и при условии надлежащего исполнения Стороной-1 своих обязательств по Договору, Сторона-1 имеет право требовать от Стороны-2 уплаты неустойки в размере 0,1 % от суммы подлежащей оплате за каждый рабочий день просрочки, но не более 5 (пяти) % от общей стоимости Договора.

**6.5.** Требование об уплате неустойки, предусмотренной п.6.4 Договора должно быть оформлено в письменном виде, подписано уполномоченным представителем. В случаях, установленных в п. 6.2, 6.3. Договора, Сторона-2 направляет Стороне-1 уведомление об удержании из суммы, подлежащей оплате или из суммы гарантийного обеспечения исполнения договора неустойки в письменном виде за подписью уполномоченного лица.

**6.6.** Уплата неустойки не освобождает Стороны от исполнения своих обязательств по настоящему Договору.

**7. Форс-мажор**

* 1. Стороны освобождаются от ответственности, за частичное или полное неисполнение обязательств по настоящему Договору, при условии соблюдения условий настоящего раздела Договора, если это неисполнение явилось следствием обстоятельств непреодолимой силы (форс-мажор), которые соответствующая Сторона не могла ни предвидеть, ни предотвратить разумными мерами при той степени добросовестности, осмотрительности и заботливости, какая от нее требовалась по характеру соответствующего обязательства.
  2. К обстоятельствам непреодолимой силы относятся следующие, но не ограничиваются ими: наводнение, пожар, землетрясение, взрыв, шторм, оседание почвы и иные явления природы, эпидемии, а также война или военные действия, массовые беспорядки, принятие органами государственной власти или управления решения, акта, повлекшего невозможность исполнения настоящего Договора, в т. ч. наложение ареста на имущество/расчетные счета Сторон.
  3. В случае, когда форс-мажорные обстоятельства преодолены, действие настоящего Договора продлевается на срок, равный по продолжительности периоду действия форс-мажорных обстоятельств.
  4. О наступлении форс-мажорных обстоятельств, а также о предполагаемом сроке их действия, Сторона, для которой такие обстоятельства наступили, извещает в письменной форме другую Сторону, по возможности немедленно, но не позднее 5 (пяти) рабочих дней с момента их наступления. При отсутствии возможности отправить извещение в письменной форме, извещение подлежит отправлению в электронном виде на следующие электронные адреса: [InfSecurity@megacom.kg](mailto:__________@megacom.kg) и [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_](file:///\\megacom.local\root\Бишкек\Департамент%20информационных%20технологий\Отдела%20закупок%20и%20учета%20оборудования%20ИТ\Закупки\2022\ТО\eostapyuk@megacom.kg). Не извещение или несвоевременное извещение о наступлении таких обстоятельств лишает права ссылаться на форс-мажорные обстоятельства.
  5. Если форс-мажорные обстоятельства продолжаются более 3 (трех) месяцев подряд, любая из Сторон вправе расторгнуть настоящий Договор, уведомив другую Сторону об этом не менее чем за 10 (десять) рабочих дней до расторжения.
  6. Сторона, ссылающаяся на форс-мажорные обстоятельства, в течение 30 (тридцати) календарных дней с момента окончания обстоятельств непреодолимой силы, обязана предоставить для подтверждения их наступления и прекращения другой Стороне документ соответствующего компетентного органа (для КР – Торгово-промышленная палата). Разумность сроков в данном случае определяется порядком документооборота соответствующего компетентного органа.

**8. Разрешение споров**

* 1. Стороны договорились разрешать любые споры, возникающие в связи с исполнением настоящего Договора, путем переговоров.
  2. Все претензии Сторон должны быть оформлены в письменном виде и подписаны уполномоченными лицами.
  3. Сторона, получившая претензию, обязана предоставить другой Стороне мотивированный ответ в течение 10 (Десяти) рабочих дней со дня получения претензии.
  4. Если Сторонам не удается найти взаимоприемлемого решения, спор подлежит разрешению в судебном порядке в судах общей юрисдикции Кыргызской Республики в соответствии с действующим законодательством Кыргызской Республики.

**9. Конфиденциальность**

* 1. Стороны согласились, что условия настоящего Договора, факт его заключения, коммерческая, финансовая, технологическая, техническая информация (вне зависимости от способа предоставления) и иная информация,  относящаяся прямо или косвенно к одной из сторон, которая ее раскрывает (далее Передающая сторона), а также любая другая информация, ставшая известной Сторонам в ходе исполнения настоящего Договора является Конфиденциальной информацией и предназначена исключительно для пользования Сторонами в целях надлежащего исполнения настоящего Договора.
  2. Каждая из Сторон обязуется соблюдать конфиденциальность в отношении информации, полученной от другой Стороны (далее Получающая сторона) и не разглашать ее третьим лицам без получения письменного согласия Передающей стороны.
  3. Стороны обязуются в течение срока действия настоящего Договора и в течение 5 (пяти) лет после его прекращения хранить в тайне Конфиденциальную информацию.
  4. Требования п. 9.1. Договора не распространяются на информацию, которая:

- на момент разглашения являлась общеизвестной/общедоступной информации во время ее получения;

- была получена в любое время из другого источника без каких-либо ограничений относительно ее распространения или использования;

- была известна Получающей стороне или находилась в ее распоряжении до ее получения;

- подлежит разглашению в соответствии с требованием и/или предписанием соответствующего государственного органа на основании законодательства КР.

**10. Расторжение договора**

**10.1.** Сторона-2 имеет право отказаться от исполнения настоящего Договора полностью или частично в одностороннем порядке с предварительным уведомлением Стороны-1 за 10 (десять) календарных дней до предполагаемой даты расторжения.

**11. Гарантии Сторон**

**11.1.** Каждая из Сторон, заключая настоящий Договор, подтверждает и гарантирует, что:

**11.1.1.** Является действующей по законодательству Кыргызской Республики, должным образом зарегистрированной и поставленной на учет во все компетентные государственные органы Кыргызской Республики;

**11.1.2.** Лицо, заключающее настоящий Договор от ее имени, обладает всеми необходимыми полномочиями на его заключение на момент подписания настоящего Договора;

**11.1.3.** Предоставленная друг другу информация является достоверной и сообщена в объеме, необходимом для надлежащего исполнения условий настоящего Договора, без каких-либо изъятий, искажений и неточностей;

**11.1.4.** Не имеет ограничений и запретов, препятствующих, ограничивающих и/или делающих невозможным заключить настоящий Договор;

**11.2.** Каждая Сторона самостоятельно несет ответственность за нарушение п. 11.1 настоящего Договора, а также за последствия, наступившие ввиду такого нарушения.

**11.3.** Каждая Сторона самостоятельно несет ответственность за своевременное оформление и продление сроков действия всех необходимых разрешений/лицензий и иных документов, необходимых для осуществления деятельности, предусмотренной настоящим Договором.

**12. Заключительные положения**

**12.1.** Настоящий Договор вступает в силу с момента его подписания обеими Сторонами и действует до полного исполнения Сторонами своих обязательств по нему.

**12.2.** Изменения и дополнения к настоящему договору действительны только в том случае, если составлены в письменной форме и подписаны обеими сторонами.

**12.3**. Настоящий Договор составлен в двух экземплярах, по одному экземпляру для каждой стороны, которые имеют одинаковую юридическую силу.

**12.4.** Договор, приложения и дополнительные соглашения к нему, а также документы, составленные во исполнение настоящего Договора, могут быть подписаны с использованием факсимильного воспроизведения подписи либо иного аналога собственноручной подписи.

**12.5.** Все уведомления, запросы, требования или любая другая корреспонденция по настоящему Договору выполняются в письменной форме на русском языке и доставляются курьером или предоплаченным заказным почтовым отправлением, а в случаях, когда корреспонденция предусмотрена настоящим Договором посредствам электронной почты, такая корреспонденция направляется по следующим адресам:

**А. Электронный адрес от Стороны-1:**

*-* ***\_\_\_\_\_\_\_\_\_\_\_\_\_****; Tел.: \_\_\_\_\_\_\_\_\_\_\_\_\_; Эл. почта:*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*;*

**Б. Электронный адрес от Стороны-2:**

***- ОИТБ*** [***InfSecurity@megacom.kg***](mailto:InfSecurity@megacom.kg)

**12.6.** Ни одна из сторон не может передавать свои права и обязательства по Договору третьим лицам без письменного согласия другой стороны.

**12.7.** Во всем остальном, что не предусмотрено настоящим Договором, стороны руководствуются действующим законодательством Кыргызской Республики

**13. Юридические адреса и реквизиты сторон:**

|  |  |
| --- | --- |
| **Сторона-1** | **Сторона-2** |
|  | **ЗАО "Альфа Телеком"**  г. Бишкек, ул. Суюмбаева, 123.  Р\С: 1091820182530113  Бишкекский центральный филиал  ОАО "Оптима Банк",  БИК: 109018  SWIFT: ENEJKG22  **Для перечисления ГОИД:**  ОАО «Айыл Банк»,  г. Бишкек, Кыргызская Республика  ЗАО "Альфа Телеком",  Счет № 1350100027537623  БИК: 135001 |
| **Директор**  **/\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  М.П. | **Генеральный директор**  **/Мамытов Н. Т./\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  М.П. |

**Приложение №1**

**к Договору о предоставлении прав доступа к технической поддержке № \_\_\_\_\_**

**от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2022г.**

**Спецификация**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Подробное описание** | **Срок действия прав доступа к технической поддержке** | **Кол-во лицензий** | **Стоимость (без учета НДС), Сом КР** | **НДС 12%,**  **Сом КР** | **Итого стоимость с учетом налогов, Сом КР** |
| 1 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | С даты подписания акта приема-передачи, сроком на 12 месяцев. | 400 |  |  |  |
|  | **Итого, общая сумма составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сомов, в том числе сумма НДС 12% составляет **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сом. | | | | | | |

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Директор  \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. | **Сторона-2:**  **ЗАО "Альфа Телеком"**  Генеральный директор  Мамытов Н.Т. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. |

**Приложение №2**

**к Договору о предоставлении прав пользования технической поддержкой № \_\_\_\_\_\_\_**

**от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2022 г.**

**г. Бишкек**

**Акт**

**приема-передачи прав доступа к технической поддержке**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** в дальнейшем именуемое «**Сторона-1**», в лице директора**\_\_\_\_\_\_\_\_\_**, действующего на основании Устава, с одной стороны, и

и ЗАО **«Альфа Телеком»**, именуемое в дальнейшем Сторона-2, в лице Генерального директора Мамытова Н.Т., действующего на основании Устава, с другой стороны, вместе именуемые — Стороны, а каждое по отдельности — Сторона, составили настоящий Акт приема-передачи о нижеследующем:

1. Сторона-1 предоставила Стороне-2 право доступа к программному обеспечению, лицензиям и технической поддержке следующего программного обеспечения:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование услуг** | **Подробное описание** | **Срок действия прав доступа к технической поддержке** | **Кол-во, лицензий** | **Стоимость (без учета НДС), Сом КР** | | **НДС, Сом КР** | | **Итого, с учетом налогов (Сом КР)** | | |
|  | | | | | | | | | | | |
|  |  |  |  |  | |  | |  | | |  |
|  | **ИТОГО:** | | | | | | | | |  | |

**2.** Стороны претензий друг к другу не имеют.

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Директор  \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. | **Сторона-2:**  **ЗАО "Альфа Телеком"**  Генеральный директор  Мамытов Н.Т. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. |

**Форма согласована:**

|  |  |
| --- | --- |
| **Сторона-1:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Директор  \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. | **Сторона-2:**  **ЗАО "Альфа Телеком"**  Генеральный директор  Мамытов Н.Т. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. |