Техническая спецификация

по лоту:

Работы по установке/монтажу систем безопасности и аналогичных систем (Работы по внедрению Системы предотвращения утечек информации (Data Leakage Prevention))

1. Определения и сокращения

Перехват – негласное копирование отправляемой, получаемой, отображаемой и вводимой информации.

Документ – объект, содержащий информацию в любом виде.

Рабочие станции – персональные компьютеры, ноутбуки и т.д.

2. Общие положения

2.1. Система предотвращения утечек информации (Далее – **Система**) должна обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей. **Система** должна анализировать все данные, передаваемые работниками как внутри, так и за пределы информационной сети Заказчика.

2.2. Информационная сеть Заказчика включает в себя 400 рабочих станций пользователей.

3. Требования к проведению работ

3.1. Дистрибутив программного обеспечения должен поставляться с документацией в электронном или печатном виде на государственном и/или русском языке. Документация должна включать в себя правила установки и использования Лицензионного программного обеспечения.

3.2. Исполнитель должен предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие права на обновление и поддержку (гарантийное сопровождение) программного обеспечения в течение 12 (двенадцати) месяцев с момента подписания акта выполненных работ.

3.3. Предоставление Заказчику прав пользования на внедряемую **Систему** не должно нарушать никаких прав третьих лиц.

3.4. Исполнитель обязуется передать Заказчику оригинал документа от производителя, подтверждающего права Заказчика на бессрочное пользование **Системой**.

3.5. Исполнитель обязуется передать лицензионные ключи в электронном виде на внедряемую **Систему**.

3.6. Внедряемая **Система** должна отвечать требованиям закона Республики Казахстан «Об авторском праве и смежных правах».

4. Программное обеспечение должно включать следующие модули:

№ п/п	Наименование программного обеспечения
1.	модуль индексации
2.	модуль контроля электронной почты (в том числе передаваемой по защищенным каналам, а также входящей/исходящей почты через web-интерфейс) с функцией остановки
3.	модуль контроля сервисов обмена мгновенными сообщениями, в том числе социальных сетей
4.	подсистема контроля HTTP-трафика (POST- и GET-запросы)
5.	модуль контроля печати
6.	модуль контроля и управления доступом съемных устройств
7.	модуль индексации файлов рабочих станций
8.	модуль контроля событий на мониторах сотрудников
9.	модуль контроля данных, вводимых с клавиатуры
10.	модуль хранения данных
11.	модуль принятия решений
12.	модуль администрирования
13.	модуль контентного анализа
14.	модуль сбора статистики и предоставления отчетов
15.	модуль расследования инцидентов

5. Технические требования к Системе

5.1. Требования к системе в целом:

1) **Система** должна поддерживать контроль следующих данных:
   a) электронной почты по протоколам: POP3, IMAP, MAPI, веб-почта, SMTP с возможностью активации/деактивации функции остановки;
   b) сервисов обмена мгновенными сообщениями (ICQ, QIP, MSN, Mail.ru Agent, Yahoo Messenger, Jabber и т.п.), клиентских программ Microsoft Lync и Viber Desktop, а также чаты социальных сетей (Facebook, Одноклассники, LinkedIn, ВКонтакте и др.);
   c) веб-запросов интернет-форумов, блогов, чатов, служб веб-почты, браузерных IM-клиентов;
   d) съемных устройств;
   e) отправленных на печать документов;
   f) событий на мониторах;
   g) данных, вводимых с клавиатуры (в том числе нажатия системных клавиш и их сочетаний);
   h) содержимого документов на рабочих станциях пользователей.
2) **Система** должна предполагать возможность установки отдельного модуля по каждому из вышеперечисленных каналов передачи данных.
3) **Система** должна иметь удобный и понятный пользовательский интерфейс, где все сообщения и документация должны быть на государственном и/или русском языке.
4) **Система** не должна накладывать ограничений на нормальное функционирование серверов и рабочих станций Заказчика.
5) **Система** должна обеспечивать разграничение прав доступа к перехваченной информации и настройкам системы.
6) **Система** должна обеспечивать перехват шифрованного трафика как на уровне рабочих станций, так и на уровне сетевых шлюзов.
7) **Система** должна обладать возможностью оптимизации нагрузки на ресурсы территориально разделенных сетей с «узким» каналом передачи данных благодаря предварительному сжатию информации, настройке расписания и скорости ее передачи.
8) **Система** должна обеспечивать блокировку HTTP и HTTPS-трафика согласно настраиваемым правилам с учетом таких атрибутов как: дата, доменное имя пользователя, IP-адрес, HTTP-метод, текст запроса и др.
9) Агент **Системы**, осуществляющий перехват на уровне рабочих станций, должен быть подписан цифровой подписью для обеспечения его целостности и предотвращения возможности встраивания в него стороннего или вредоносного кода.
10) **Система** не должна ухудшать основные функциональные характеристики ИС (надежность, быстродействие, возможность изменения конфигурации, удобство использования).
11) **Система** должна обладать характеристиками масштабирования и отказоустойчивости.
12) **Система** должна обеспечить интеграцию в существующую у Заказчика вычислительную сеть без изменения топологии сети.
13) **Система** должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах.
14) Все функции **Системы** должны выполнятся в рамках единого решения, единой СУБД для перехваченных данных, вердиктов и работать в рамках одной линейки операционных систем. Исключением служат сторонние сервисы, с которыми **Система** имеет возможность интеграции.

5.1.1. Требования к структуре и функционированию **Системы**

1) Структурно **Система** должна включать следующие компоненты:
   - сервер индексации;
   - сервер сетевого перехвата и/или сервер перехвата на рабочих станциях;
   - сервер хранилища данных;
   - модуль сбора статистики и формирования отчетов;
   - модуль администрирования;
   - модуль интеграции с сервисом экспертизы изображений;
   - модуль принятия решений;
   - модуль расследования инцидентов.
2) В состав **Системы** должны входить следующие основные логические модули:
   - модуль контроля почтового трафика;
   - модуль контроля сервисов обмена мгновенными сообщениями;

- модуль контроля HTTP-трафика;
- модуль контроля печати;
- модуль контроля съёмных устройств;
- модуль контроля событий на мониторах сотрудников;
- модуль контроля данных, вводимых с клавиатуры;
- модуль индексации;
- модуль индексации файлов рабочих станций;
- модуль хранения данных;
- модуль принятия решений;
- модуль контентного анализа;
- модуль администрирования;
- модуль сбора статистики и предоставления отчетов;
- модуль расследования инцидентов.

3) Модуль контроля почтового трафика должен обеспечивать перехват сообщений электронной почты (протоколы SMTP/ESMTP, POP3. IMAP, MAPI, веб-почта), также иметь функцию автоматической остановки отправки сообщения в случае возникновения инцидента на конечных станциях или почтовом сервере.
4) Модуль контроля сервисов обмена мгновенными сообщениями должен обеспечивать перехват сообщений и файлов, переданных при помощи интернет-мессенджеров, а также чаты, звонки и файлы клиентских приложений Microsoft Lync и Viber Desktop.
5) Модуль контроля HTTP-трафика должен обеспечивать контроль POST- и GET-запросов при использовании пользователями Заказчика интернет-сервисов, также иметь подключаемую функцию автоматической остановки траффика в случае возникновения инцидента.
6) Модуль контроля печати должен обеспечивать контроль документов, отправленных на печать при помощи сетевых или локальных принтеров.
7) Модуль контроля съемных устройств должен обеспечивать контроль файлов, записываемых на USB-устройства, CD-/DVD-матрицы и др. типы съемных устройств.
8) Модуль контроля событий на мониторах сотрудников должен обеспечивать контроль изображений с экранов пользователей, возможность вести видеозапись действий, а также предоставлять возможность просмотра содержимого мониторов пользователей в режиме реального времени.
9) Модуль контроля данных, вводимых с клавиатуры должен осуществлять логирование нажатий клавиш в любых приложениях (в том числе нажатия системных клавиш и их сочетаний).
10) Модуль индексации должен обеспечивать индексирование документов, перехваченных модулями контроля, для быстрого поиска по ним в дальнейшем.
11) Модуль индексации файлов рабочих станций сети должен обеспечивать контроль всех документов, располагающихся на рабочих станциях локальной сети.
12) Модуль хранения должен обеспечивать запись почтовых сообщений, сообщений интернет-мессенджеров, HTTP и HTTPS трафика, мгновенных сообщений Viber и Lync, отправленных на печать документов, записанных на съемные носители файлов, перехваченных разговоров, данных об активности процессов и данных, вводимых с клавиатуры, в базы данных под управлением Microsoft SQL Server 2008 R2 и версий выше.
13) Модуль принятия решений должен предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту – нарушает или не нарушает он существующие правила. А в случае с перехватом объекта по протоколу SMTP, выносить вердикт о внесении или не внесении письма в карантин и остановки отправки сообщения (до расследования события сотрудником, ответственным за информационную безопасность).
14) Модуль контентного анализа должен предоставлять возможность проведения ретроспективного анализа перехваченной информации, учитывая возможность изменения правил проверки.
15) Модуль администрирования должен обеспечивать управление настройками конфигурации **Системы** и обеспечивать 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 верной работоспособности всех компонентов **Системы** и автоматическое уведомление администратора в случае нештатных ситуаций.
16) Модуль сбора статистики и предоставления отчетов должен производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности.

17) Модуль расследования инцидентов должен предоставлять помощь сотруднику службы безопасности в категоризации фактов нарушений информационной безопасности компании, ведении «Дел» по сотрудникам и проведении расследований.

5.1.2. Требования к способам и средствам связи для информационного обмена

1) Внедряемая **Система** должна функционировать на существующем основном оборудовании заказчика в составе информационно-вычислительной сети Заказчика:
2) Все компоненты **Системы** должны работать на платформе Microsoft Windows.
3) **Система** должна корректно работать в сетях с доменом Active Directory.
4) **Система** должна поддерживать виртуальную инфраструктуру (VMware ESX/ESXi).
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 приема-передачи данных между **Системой** и корпоративной почтовой системой должен использоваться протокол SMTP.
7) Должна использоваться единая точка съема почтового, HTTP и HTTPS-трафика.

5.1.3. Требования к характеристикам взаимосвязей

1) Предусмотреть взаимодействие доменов и поддоменов, как связанных, так и не связанных отношениями доверия.
2) Предусмотреть взаимодействие корпоративных почтовых серверов Заказчика с **Системой** через механизмы ретрансляции почтового трафика SMTP-relay.
3) Предусмотреть 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).

5.1.4. Требования к режимам функционирования **Системы**

Основной режим функционирования **Системы** – автоматический, под управлением администратора. **Система** должна обеспечивать возможность работы в следующих режимах:

- штатный режим (непрерывная круглосуточная работа);
- сервисный режим (для проведения обслуживания, реконфигурации и модернизации компонент);
- автономный режим (в случае отсутствия связи между компонентами системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

5.1.5. Требования по диагностированию **Системы**

1) **Система** должна делать записи в служебные журналы информацию о служебных событиях и сбоях. Записи в служебных журналах должны содержать информацию, достаточную для установления причины неисправности.
2) Каждый модуль системы должен иметь штатный и расширенный режим записи в журналы отладки. В случае программных сбоев должен быть предусмотрен отладочный режим принудительной записи в журналы отладки. 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.

5.1.6. Возможности, касающиеся развития и модернизации **Системы**

1) **Система** должна быть реализована как масштабируемая система и допускать наращивание производительности за счет улучшения характеристик технических средств.
2) **Система** должна обеспечивать возможность модернизации путем замены оборудования и/или программного обеспечения.

5.1.7. Требования к надежности

1) Должна быть обеспечена непрерывность бизнес-процессов Заказчика в случае отказов **Системы**.
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 (предпочтительно) в срок не более 6 часов.

3) В случае возникновения сбоя технического или программного обеспечения **Системы** должна быть обеспечена возможность восстановления ее данных и настроек.
4) Процедуры восстановления работоспособности **Системы** должны быть описаны и задокументированы в соответствующей эксплуатационной документации на Систему.

5.2. Общие требования к функциям (задачам)

5.2.1. Требования к модулю контроля почтовых сообщений

1) Модуль должен предоставлять возможности для контроля сообщений и вложений, переданных по протоколам SMTP, POP3, IMAP, MAPI, HTTP, HTTPS (веб-почта: как исходящая, так и входящая) при помощи любых почтовых клиентов или браузеров. Иметь подключаемую функцию автоматической остановки исходящего SMTP, HTTP и HTTPS трафика в случае возникновения инцидента.
2) Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.
3) Модуль должен обеспечивать помещение перехваченных документов в базу данных под управлением СУБД Microsoft SQL Server.
4) Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулю контентного анализа и модулю принятия решений для вынесения вердикта.
5) Модуль должен предоставлять средства интеграции с прокси-серверами по протоколу ICAP.
6) Модуль должен обеспечивать интеграцию как с аппаратными, так и с программными прокси-серверами для перехвата HTTPS-траффика (MS ISA/TMG, Kerio Control, Squid и др.).
7) Модуль должен предоставлять средства интеграции с корпоративными почтовыми серверами (Lotus Domino, Microsoft Exchange и др.).
8) Модуль должен обеспечивать SMTP-интеграцию с корпоративными почтовыми серверами, поддерживающими функцию журналирования.

5.2.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

1) Модуль должен обеспечивать перехват входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), MSN (MSN/Windows Live Messenger), XMPP (Jabber, Google Hangouts), MMP (Агент Mail.ru), SIP (X-Lite и др.), YAHOO (Yahoo! Messenger), Gadu-Gadu, а также входящие и исходящие сообщения по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Google+, Мамба.ru и прочее) и сообщения веб-версии Skype (web.skype.com).
2) Модуль должен обеспечивать перехват входящих/исходящих сообщений, звонков и файлов клиентских программ Microsoft Lync и Viber.
3) Модуль должен обеспечивать перехват 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.
5) Модуль должен обеспечивать помещение перехваченных документов в базу данных под управлением СУБД Microsoft SQL Server.
6) Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.

5.2.3. Требования к модулю контроля HTTP-трафика

1) Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).
2) Модуль должен поддерживать перехват HTTP-запросов, поступающих от ICAP-сервера.
3) Модуль должен поддерживать фильтрацию запросов, генерируемых всеми современными браузерами, в том числе Internet Explorer 6+; Mozilla Firefox 2+; Opera 8+; Google Chrome 8+.
4) Модуль должен поддерживать перехват GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.
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 обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

8) Модуль должен обеспечивать помещение перехваченных документов в базу данных под управлением СУБД Microsoft SQL Server.
9) Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.

5.2.4. Требования к модулю контроля печати

1) Модуль должен осуществлять перехват документов, отправленных на печать при помощи локальных и сетевых принтеров.
2) Модуль должен осуществлять перехват 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 сетевого перехвата отдельных принтеров.
5) Модуль должен поддерживать возможность исключения из сетевого перехвата отдельных документов по их именам.
6) Модуль должен позволять блокировку Escape-функций для PostScript/PCL принтеров, при активации которых перехват распечатанных документов невозможен.
7) Модуль должен обеспечивать помещение перехваченных графических и текстовых представлений документов в базу данных под управлением СУБД Microsoft SQL Server.
8) Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.

5.2.5. Требования к модулю контроля съёмных устройств

1) Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (CD-/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, PCMCIA, 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 предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе.
6) Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».
7) Модуль должен предоставлять возможность ограничивать теневое копирование, исходя из формальных признаков файлов (доменное имя, формат).
8) Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя.
9) Модуль должен предоставлять возможность контроля и блокировки буфера обмена на компьютере пользователя.
10) Модуль должен предоставлять возможность блокировки доступа пользователей к определенным папкам и/или всем логическим дискам (за исключением системных).
11) Модуль должен предоставлять возможность использования «белых списков» устройств, к которым в дальнейшем пользователь будет иметь неограниченный доступ.
12) Модуль должен предоставлять возможность шифрования данных, записываемых на USB-устройства. Настройки шифрования должны позволять задать правила, в которых можно выбрать пользователей/группу пользователей, записываемые данные которых будут зашифрованы, а также пользователей/группу пользователей, доступ к зашифрованным данным для которых будет разрешен либо заблокирован.
13) Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.
14) Модуль должен обеспечивать помещение перехваченных документов в базу данных под управлением СУБД Microsoft SQL Server.
15) Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулям контентного анализа и принятия решений для вынесения вердикта.

5.2.6. Требования к модулю контроля событий на мониторах 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 позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, звонке или активации видеоконференции Skype, при блокировке компьютера или отсутствии активности от клавиатуры и мыши.
3) Модуль должен обеспечивать видеозапись происходящего на экранах мониторов согласно настроенному расписанию или событиям.
4) Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи.
5) Модуль должен обеспечивать одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени.
6) Модуль должен обеспечивать помещение перехваченных документов в базу данных под управлением СУБД Microsoft SQL Server.
7) Модуль должен предоставлять возможность экспорта перехваченных снимков экрана и видеозаписей в отдельную папку.

5.2.7. Требования к модулю контроля данных, вводимых с клавиатуры

1) Модуль должен обеспечивать перехват нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.
2) Модуль должен обеспечивать перехват текстовой информации, помещенной пользователем в буфер обмена.
3) Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.
4) Модуль должен обеспечивать помещение перехваченной информации в базу данных под управлением СУБД Microsoft SQL Server.
5) Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулю анализа и принятия решений для вынесения вердикта.
6) 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.
7) Модуль должен предоставлять возможность экспорта перехваченных нажатий клавиш в отдельную папку.

5.2.8. Требования к модулю индексации рабочих станций

1) Модуль должен обеспечивать индексирование баз данных **Системы** и сторонних баз данных.
2) Модуль должен обеспечивать подключение внешних источников данных для индексации.

5.2.9. Требования к модулю индексации файлов рабочих станций

1) Модуль должен обеспечивать отслеживание изменений файлов и высокую частоту переиндексации информации (отслеживание и переиндексацию только новых и измененных файлов).
2) Модуль должен обеспечивать возможность сохранения теневой копии данных, в случае, если те умышленно удалены пользователем.

5.2.10. Требования к модулю хранения данных

1) Модуль должен обеспечивать архивирование следующих данных:
   a) почтовых сообщений и вложенных в них файлов;
   b) сообщений и файлов IM-клиентов;
   c) сообщений, звонков и файлов клиентского приложения Microsoft Lync и Viber;
   d) HTTP-запросов (сообщения и файлы);
   e) сеансов текстовой и голосовой связи, файлов и SMS-сообщений, переданных или полученных по Skype;
   f) графических представлений и текста отправленных на печать документов;
   g) журнала аудита внешних устройств, где фиксируются данные об операциях, выполняемых на подключаемых внешних устройствах;

h) информации, содержащей перехваченные нажатия клавиш, и текстовую информацию, помещенную в буфер обмена;
i) аудиозаписей перехваченных разговоров пользователей;
j) зафиксированных операций с файлами;
k) входящих и исходящих данных облачных сервисов;
l) данных об активности пользователей и приложений;
m) перехваченных снимков экрана пользователя в графическом формате.

2) Для архивирования перехваченных данных, **Система** должна использовать базы под управлением Microsoft SQL Server 2008 R2 или выше. Модуль должен архивировать все перехваченные объекты, а не только те, по которым зафиксированы инциденты.

5.2.11. Требования к модулю принятия решений

1) Модуль должен использовать два пользовательских приложения: консоль сервера для задания настроек и клиентскую консоль для управления политиками безопасности, инцидентами и карантином.
2) Модуль должен выносить единый вердикт (инцидент / не инцидент) для каждого перехваченного объекта.
3) Модуль должен предоставлять возможности для ведения журнала инцидентов с возможностью рубрикации по каналам передачи данных, протоколам, пользователям, правилам проверки.
4) Модуль должен предоставлять возможность уведомления ответственных лиц об инцидентах по электронной почте.
5) Модуль должен предоставлять возможность блокировки (помещения в карантин) SMTP-трафика электронной почты до принятия вердикта ответственным лицом.
6) Модуль должен предоставлять возможности для задания правил автоматического вынесения вердикта по объекту (инцидент / не инцидент). Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:
   a) формальных признаков перехваченного объекта (доменное имя, отправитель, получатель, хост, размер, расширение файла, канал передачи данных, протокол и т.д.);
   b) защищенных паролем файлов и архивов;
   c) 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).
7) Модуль должен предоставлять возможности для изменения существующих и применения новых правил автоматического вынесения вердикта.
8) Модуль должен предоставлять возможность выполнения ретроспективного контроля перехваченных документов с учетом обновленных правил проверки.
9) Модуль должен предусматривать возможность объединения политик безопасности (правил проверки) в группы.
10) Модуль должен предоставлять возможность задания для каждой группы политик безопасности индивидуальных настроек: перечня индексов, по которым будет проводиться опрос, расписания проверки, списка получателей оповещений об инцидентах, списка исключений.
11) Модуль должен предоставлять возможности для использования «белых списков» (списки пользователей, документы которых исключены из проверок) и «черных списков» (списки пользователей, только по документам которых будет проводиться проверка).
12) Модуль должен предоставлять возможность экспорта/импорта структуры настроек (политик безопасности, критериев поиска, списков исключений и др.).
13) Модуль должен 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.
14) Модуль должен предоставлять возможности протоколирования выявленных инцидентов.
15) Модуль должен поддерживать возможность категоризации инцидентов с помощью цветовых меток.
16) Модуль должен предоставлять возможности для принятия решений в отношении следующих типов объектов:
   a) сообщений, переданных по поддерживаемым **Системой** каналам и протоколам;
   b) 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);

c) распознанных и проанализированных текстов в графических файлах форматов bmp, jpg, jpeg, png, tif, tiff, gif;

d) документов, вложенных в сжатые файлы: rar, zip, 7z, jar, tar, arj, gz, gzip, cab, iso, chm, hlp, 001.

17) Модуль должен обеспечить наличие следующих возможностей обнаружения критичной информации:

a) по ключевым словам, в том числе с возможностью ограничений по взаимному расположению искомых слов и с учетом морфологических особенностей и синонимии русского языка;

b) возможность обнаружения похожих документов на основе образца, схожего по содержанию и смыслу с искомым;

c) 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;

d) по заранее заданному словарю с целью выявления определенных типов документов (резюме, финансовые и бухгалтерские отчеты);

e) 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;

f) 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;

g) по цифровым отпечаткам конфиденциальных документов (включая вложенные файлы), с возможностью указания порога срабатывания;

h) по значениям атрибутов баз данных (как общих атрибутов, так и уникальных для отдельных продуктов);

i) по количественным показателям статистических запросов (числу отправленных писем/распечатанных страниц/сообщений в Skype, Lync, Viber, IM и пр.);

j) по цепочкам событий или событиям с определенной продолжительностью (попытка подбора учетной записи, создание временной учетной записи, временное включение учетной записи и др.);

k) возможность сузить результаты поиска путем дополнительного поискового запроса (фильтры по найденному).

18) Модуль должен предусматривать наличие в дистрибутиве словарей на государственном и/или русском языке.

19) Модуль должен обеспечивать устойчивость к следующим видам манипуляции с информацией:

a) импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными;

b) изменение порядка слов;

c) изменения расстояний между словами;

d) изменение форматирования документа;

e) изменение словоформ;

f) замены букв на символы другого алфавита;

g) использование цифр вместо букв;

h) изменение расширений файлов.

20) Модуль должен предоставлять возможности для просмотра детальной информации по каждому инциденту.

5.2.12. Требования к модулю контентного анализа

1) Модуль контентного анализа должен быть ориентирован на работу с индексами и базами данных модулей контроля информации.

2) Модуль должен предоставлять возможность выполнять ретроспективный анализ всех перехваченных или запротоколированных объектов, означенных в п. 4.2:

- поиск по ключевым словам и фразам в базах перехваченных документов;
- выборка перехваченных данных по дате, доменному имени, адресам и хостам электронной почты, 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 (словарю), 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.

3) Модуль должен предоставлять возможности для просмотра детальной информации по каждому перехваченному объекту.
4) Модуль должен позволять просматривать записи действий на экранах пользователей во встроенном видеоплеере, а также соотносить видеозаписи с активностью приложений и нажатиями клавиш.
5) Анализ текстового содержимого должен производиться с учетом морфологических особенностей и синонимов русского языка. При этом словоформы должны образовываться без использования логических операторов и специальных символов.
6) Модуль должен предоставлять возможности экспорта выборки перехваченных данных полного списка или набора файлов с оглавлением.
7) Модуль должен 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 ICQ, MSN и других IM-клиентов), а также информацию по связям текущего пользователя за указанный период времени.
8) Модуль должен предоставлять возможность подготовки отчетов по результатам выполнения пользовательской выборки.

5.2.13. Требования к модулю администрирования

1) Модуль должен предоставлять возможность контроля работоспособности **Системы**.
2) Модуль должен обеспечивать возможность управления службами модулей **Системы**.
3) Модуль должен предоставлять возможность управления всеми индексами и базами данных модулей контроля информации.
4) Модуль должен предоставлять возможность мониторинга дискового пространства на серверах **Системы**.
5) Модуль должен предоставлять возможность автоматического оповещения о важных событиях.
6) Модуль должен обеспечивать возможность синхронизации с одним или более доменом Active Directory.
7) Модуль должен предоставлять возможность разграничения прав доступа сотрудников службы безопасности к данным по тем или иным пользователям, группам пользователей и компьютерам. Под данными подразумеваются зафиксированные модулем принятия решений инциденты, сообщения, попавшие в карантин модуля принятия решений, а также содержимое документов при просмотре в модуле контекстного анализа.
8) Модуль должен предоставлять возможность указания настроек для подключения к базам данных, которые можно впоследствии использовать по умолчанию.
9) Модуль должен обеспечивать возможность управления настройками модулей **Системы**.

5.2.14. Требования к модулю сбора статистики и предоставления отчетов

1) Модуль должен предусматривать быстрое выполнение генерации отчетов по имеющимся шаблонам, включая сложные отчеты.
2) Модуль должен предусматривать наличие не менее 30 базовых шаблонов, а также возможность добавлять пользовательские шаблоны.
3) Модуль должен предусматривать предоставление отчетов в графическом, диаграммном, табличном виде, а также в виде временной шкалы.
4) Модуль должен производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности.

5) Модуль должен 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.
6) Модуль должен генерировать краткие и детальные отчеты по продуктивности работы пользователей за выбранный период времени.
7) Модуль должен генерировать отчеты по программам: количеству установок и удалений программ, установке/удалении агентов, перечню компьютеров с (не)установленными заданными программами и истории их изменений на компьютерах.
8) Модуль должен генерировать отчеты по устройствам: перечень установленного оборудования на компьютерах пользователей и отчет по изменениям в устройствах (комплектующих) компьютеров.
9) Модуль должен генерировать системные отчеты, отображающие:
   a) операции с агентами/протоколами, совершенные любым либо указанным пользователем;
   b) список компьютеров, выполнивших вход в домен, но не проявлявших активность;
   c) список компьютеров с нерабочими агентами;
   d) список компьютеров без агентов;
   e) список компьютеров, выполнивших вход в домен, но не имеющих установленного агента;
   f) информацию о количестве сообщений по выбранным компьютерам за заданный промежуток времени.
10) Модуль должен предоставлять возможность быстрого перехода к модулю контентного анализа для просмотра документов.
11) Модуль должен предоставлять возможность переходов по связанным отчетам.
12) Модуль должен предусматривать представление связей между внутренними и внешними адресатами в виде интерактивного графа.
13) Модуль должен обеспечивать получение наглядного представления о круге общения выбранного пользователя или нескольких пользователей.
14) Модуль должен обеспечивать получение наглядного представления о контактах внешнего адресата с сотрудниками компании.
15) Модуль должен обеспечивать получение наглядного представления об адресах, с которых выбранный пользователь отправлял либо на которые получал сообщения.
16) Модуль должен обеспечивать выявление общих адресатов для нескольких пользователей.
17) Модуль должен предусматривать возможность конвертации сгенерированных отчетов в PDF-файл, равно как и вывод их на печать.

5.2.15. Требования к модулю расследования инцидентов

1) Модуль должен предоставлять возможность ведения полноформатного расследования инцидентов в рамках одной консоли.
2) Модуль должен предоставлять возможность заведения дела на любого сотрудника Заказчика, его ведение и завершение. Для каждого отдельного дела должна быть предусмотрена возможность создания промежуточного резюме, в котором можно указать необходимую информацию о деле (например, причину его создания).
3) Модуль должен поддерживать возможность прикрепления к заведенным делам файлов, свидетельствующих о возможных инцидентах, и описаний.
4) Модуль должен поддерживать возможность категоризации (группировки) заведенных дел сотрудником службы безопасности.
5) Модуль должен поддерживать возможность работы со списком фигурантов.
6) Модуль должен предоставлять возможность просмотра истории операций с папками и делами.
7) Модуль должен поддерживать возможность вывода на печать информации по делу.
8) Модуль должен поддерживать возможность экспорта созданных дел.
9) Модуль должен поддерживать возможность переноса дела в «Архив» после завершения его расследования.

6. Требования к Исполнителю и специалистам Исполнителя

1) Для обеспечения выполнения работ по внедрению программного комплекса и запуска рабочего функционирования **Системы** в составе персонала Исполнителя должны присутствовать минимум одна штатная единица инженера технической поддержки.
2) Инженер технической поддержки должен обладать знаниями в объеме, необходимом для выполнения штатного технического и аварийного обслуживания **Системы** у Заказчика.

7. Требования по вводу в действие Системы

1) Внедрение **Системы** должно включать:
   a) обследование информационной системы
   b) подготовку к вводу **Системы** в действие
   c) установку и настройку **Системы**.
2) Исполнитель должен предоставить следующую документацию:
   a) инструкция по развертыванию и восстановлению работы **Системы**;
   b) инструкцию администратора **Системы**;
   c) инструкцию пользователя **Системы**;
   d) инструкцию по резервному копированию настроек и базы данных **Системы**.

8. Общие требования к безопасности

8.1. Согласно установленных у Заказчика процедур информационной безопасности Исполнитель и каждый специалист Исполнителя, принимающий участие в оказании услуг по Договору, должны подписать Соглашение о соблюдении правил и процедур информационной безопасности по форме, указанной в Спецификации 1. Не предоставление Заказчику соглашения, подписанного Исполнителем и специалистом Исполнителя дает право Заказчику не допускать специалистов Исполнителя к оказанию услуг. В этом случае ответственность за неоказание услуг, в связи с недопуском специалистов к оказанию услуг, несет Исполнитель.

8.2. Ответственность за защищенность информационных ресурсов от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба Заказчику или пользователям информационных ресурсов, а также за сохранность данных несет Исполнитель.

Спецификация 1 — Форма соглашения о соблюдении правил и процедур информационной безопасности

Соглашение
о соблюдении правил и процедур информационной безопасности АО «РД «КазМунайГаз»

Я, *указать фамилию имя отчество полностью*, приступая в качестве сотрудника (работника) Исполнителя (Поставщика) для АО «РД «КазМунайГаз» (далее — Заказчик) на основании Договора между Заказчиком и Исполнителем № _____ от «____» _____ 201__ года на оказание услуг:_____, принимаю на себя следующие обязательства:

1. Соблюдать относящиеся ко мне требования существующих нормативов по обеспечению информационной безопасности (далее — ИБ) Заказчика.
2. Не разглашать информацию, отнесенную к разряду коммерческой и служебной тайнам в соответствии с внутренними документами Заказчика (далее — Служебная Информация), которая мне была доверена или может стать известной при выполнении служебных обязанностей.
3. Сохранять в тайне известные мне данные по идентификации и аутентификации (пароли, ключи, способы доступа к информационным ресурсам и т. д.), обеспечивать сохранность доверенных мне Заказчиком устройств защиты информации.
4. Не подвергать угрозам целостность и доступность других видов информации, указанных в нормативных документах Заказчика.
5. Ознакомиться и строго следовать Правилам и Процедурам ИБ Заказчика.
6. Не передавать третьим лицам и не раскрывать публично Служебную Информацию Заказчика без согласования с уполномоченным контактным лицом Заказчика (далее — Куратор).
7. Оказывать содействие ответственным за ИБ в расследовании инцидентов, связанных с нарушением ИБ, и своевременно сообщать ответственным за ИБ обо всех ставших мне известными нарушениях, включая попытку посторонних лиц получить от меня Служебную Информацию.
8. Обеспечивать, в рамках своей компетенции, ИБ Служебной Информации тех организаций, с которыми Заказчик имеет деловые отношения.
9. Не использовать знания Служебной Информации для занятий любой деятельностью, которая может нанести ущерб Заказчику, во время действия настоящего Соглашения и в течение 3 (трех) лет после его окончания.
10. Передать Куратору после прекращения рабочих отношений с Заказчиком, все документы и иные материальные носители информации, содержащие Служебную Информацию, которая находилась в моем распоряжении в связи с выполнением мною рабочих обязанностей.
11. Немедленно сообщать Куратору об утрате или недостаче документов, паролей, Пин-кодов, криптографических ключей, машинных носителей и иных материальных носителей Служебной Информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению Служебной Информации Заказчика, а также о причинах и условиях возможной ее утечки.
12. Мне известно, что нарушение требований, приведенных в этих документах, может повлечь административную, гражданско-правовую и иную ответственность в соответствии с действующим законодательством Республики Казахстан.
13. Подтверждаю, что не имею иных прямых или косвенных обязательств, которые могут помешать мне исполнению настоящего Соглашения.

_____ подписано датой: «____» _____ 201__ г.
подпись, полное фамилия имя и отчество, написанное от руки

Исполнитель:

_____ *(название компании)*

_____

(БИН и юридический адрес компании)

_____

_____ *(должность руководителя)*

_____ *(подпись / ФИО руководля)*

место печати Исполнителя

Директор департамента
информационных технологий и АСУТП **Махамбетов Т. К.**