Приложение №1 к Договору №_____ от _____

УТВЕРЖДАЮ

Директор по информационным технологиям и связи
АО «ЛОЭСК»

_____ Ю.В. Матвеев

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на оказание услуг по внедрению программного обеспечения, предназначенного для предотвращения потери данных путем обнаружения возможных нарушений при их отправке и фильтрации (DLP-система).

1. Общие положения

1.1. Программное обеспечение для защиты информации (Далее – Система) должно 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 АО «ЛОЭСК» (далее – Заказчик).

1.2. Информационная сеть Заказчика включает в себя 800 рабочих станций пользователей, является территориально распределенной на территории Ленинградской области. Центр обработки данных и управления сетью расположен по адресу Санкт-Петербург, Песочная наб., 42А.

1.3. В рамках проекта реализуются следующие этапы:

- комплекс консультационных услуг с последующей подготовкой правовой и организационной документации в соответствии с настоящим Техническим заданием;
- передача ЗАКАЗЧИКУ неисключительных прав на использование программ для ЭВМ;
- передача ЗАКАЗЧИКУ документа (сертификата правообладателя), удостоверяющего право Заказчика на получение от правообладателя услуг по технической поддержке программного обеспечения в течение 3-х лет.
- услуги по установке и настройке ПО.

2. Требования к этапу обследования

2.1. На этапе обследования Исполнителем услуги должны быть произведены следующие работы:

- подготовка анкеты (опросного листа), отражающей отраслевую специфику, для заполнения кураторами информационных ресурсов Заказчика, а также руководства по заполнению опросных листов;
- разработка классификатора критичных информационных активов (информации ограниченного доступа);
- разработка правил обработки информации ограниченного доступа (включая создание, хранение, изменение, доступ, использование, перемещение, удаление), обрабатываемой в подразделениях Заказчика;
- разработка комплекта документов для обеспечения юридической значимости системы мониторинга и контроля (Системы):
    - Положение о порядке обращения с информацией ограниченного доступа (включает правила обработки);
    - Положение о защите информации ограниченного доступа;
    - Положение о мониторинге и контроле;
    - Соглашение о неразглашении информации ограниченного доступа для сотрудников;

- Уведомление/соглашение с сотрудниками на предмет осуществления мониторинга и контроля;
- Положение о допустимом использовании ресурсов;

- проработка и документирование процедуры реагирования на инциденты, связанные с утечками информации ограниченного доступа (включая разработку технологической схемы реагирования на инциденты, связанные с утечками информации ограниченного доступа).

3. Требования к поставке лицензионных программных средств

3.1. 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. Спецификация на поставку программного обеспечения должна быть предоставлена в виде Приложения №2 к настоящему Договору.

3.2. Исполнитель должен предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие передачу прав, права на обновление и поддержку (гарантийное сопровождение) программного обеспечения в течение 12 (двенадцати) месяцев. Форму лицензионного (сублицензионного) соглашения с Заказчиком Исполнитель должен предоставить в виде Приложения №3 к настоящему Договору.

4. Технические требования к программному обеспечению

4.1. Требования к системе в целом:

Система должна поддерживать контроль следующих данных:

- электронной почты, протоколы: POP3, IMAP, MAPI, web-почта, SMTP;
- сервисов обмена мгновенными сообщениями (ICQ, Jabber), коммуникационных программ-клиентов Microsoft Lync, а также чаты социальных сетей (Facebook, Одноклассники, LinkedIn, ВКонтакте и др.);
- FTP-трафика;
- web-запросов интернет-форумов, блогов, чатов, служб web-почты, браузерных IM-клиентов;
- Skype (чаты, файлы, звонки);
- съемных устройств;
- отправленных на печать документов (локальные и сетевые принтеры);
- снимки экрана на рабочих станциях;
- облачных хранилищ данных (DropBox, Google Drive, Яндекс.Диск, Microsoft OneDrive, Evernote, SugarSync);
- содержимого файлов на жёстких дисках рабочих станций, в общих сетевых папках, а также в Microsoft SharePoint.

Система должна иметь единую консоль управления через web-интерфейс и предоставления отчетности на русском языке.

Система должна обеспечивать возможность масштабирования и отказоустойчивости.

Система должна обеспечивать возможность информирования администратора безопасности об инцидентах путем отправки письма-уведомления об инциденте на почтовый электронный адрес, а также выделением в системе инцидентов цветом, отличающимся от цвета корректных событий.

Система должна обеспечить возможность отображения снимков экранов рабочей станции связанных с событием из карточки инцидента в единой консоли.

Система должна обеспечивать возможность объединения групп, контактов, рабочих станций, веб-ресурсов в логические периметры.

Система должна обеспечивать автоматическое или ручное прикрепление ко всем инцидентам справочных данных о нарушителе, на основе данных из служб каталогов, отображение информации в системе.

Система должна обеспечивать управление загрузкой канала связи при взаимодействии с модулями Комплекса, расположенными в удаленных элементах информационной системы.

Система защиты конфиденциальной информации должна функционировать в среде следующих операционных систем:

- Microsoft Windows XP SP3
- Microsoft Windows Vista SP2
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

4.1.1. Требования к структуре и функционированию Системы

В состав Системы должны входить следующие подсистемы:

1) **Подсистема перехвата трафика** должна состоять из следующих модулей:
   - **Модуль контроля корпоративной почты**, обеспечивающий перехват, обработку и передачу на анализ почтового трафика по протоколам POP3, IMAP, MAPI и SMTP;
   - **Модуль контроля Web-трафика**, обеспечивающий перехват, обработку и передачу на анализ Web-трафика по протоколам HTTP и HTTPS;
   - **Модуль контроля программ мгновенного обмена сообщениями на рабочих станциях пользователей**, обеспечивающий перехват, обработку и передачу на анализ трафика ICQ, Skype, Jabber и Microsoft Lync, Viber и WhatsApp;
   - **Модуль контроля съемных носителей, приложений на рабочей станции**, предназначенный для контроля доступа пользователей к периферийным устройствам, контроля приложений, контроля облачных хранилищ (DropBox, Google Drive, Яндекс.Диск, Microsoft OneDrive, Evernote, SugarSync), перехвата, обработки и передачи на анализ теневых копий файлов, переносимых на съемные носители, контроля снятия снимков экрана и запуска приложений на рабочей станции, контроля доступа терминальных клиентов, подключенных к терминальному серверу посредством Microsoft RDP или Citrix ICA;
   - **Модуль контроля печати документов**, предназначенный для контроля доступа пользователей к устройствам печати, перехвата, обработки и передачи на анализ теневых копий заданий на печать;
   - **Модуль аудита хранения информации,** обеспечивающий поиск файлов, содержащих признаки конфиденциальной информации, на локальных дисках рабочих станций под управлением MS Windows, в сетевых папках, файловом хранилище MS SharePoint, и создание теневых копий найденных файлов;
   - **Модуль контроля мобильных устройств**, предназначенный для контроля сообщений и файлов, отправляемых с устройства под управлением операционных системы iOS и Android;
   - **Модуль создания снимков экрана**, предназначенный для снятия снимков экрана с рабочих станций и передачу их в подсистему хранения.
2) **Подсистема анализа** должна состоять из следующих модулей:
   - **Модуль OCR**, обеспечивающий распознавание текста, содержащегося в изображениях.
   - **Модуль лингвистического анализа**, выполняющий классификацию текста объекта путем поиска соответствия этого текста каким-либо категориям;
   - **Модуль детектирования цифровых отпечатков,** обеспечивающий поиск цитат из эталонных документов в тексте объектов;

- **Модуль детектирования текстовых объектов,** обеспечивающий поиск текстовых объектов (например, номеров кредитных карт) в тексте объектов;
- **Модуль детектирования графических объектов,** определяющий наличие изображений чертежей и топографических карт в потоке перехваченных изображений;
- **Модуль детектирования кредитных карт,** определяющий наличие изображений кредитных карт в потоке перехваченных изображений;
- **Модуль детектирования паспортов,** определяющий наличие изображений второго разворота паспорта гражданина РФ в потоке перехваченных изображений;
- **Модуль детектирования выгрузок из баз данных,** позволяющий фиксировать наличие эталонных выгрузок из баз данных в сетевом трафике и текстовых документах;
- **Модуль детектирования печатей,** позволяющий отслеживать передачу отсканированных документов, содержащих изображение эталонных печатей;

3) **Подсистема применения политик** должна состоять из следующих модулей:
   - **Модуль принятия решений,** обеспечивающий применение политики информационной безопасности путем выполнения для объектов правил из сценария обработки объектов;
   - **Модуль интеграции с Active Directory,** обеспечивающий первоначальный импорт и периодическую синхронизацию структуры каталога Active Directory со справочником сотрудников и рабочих станций для выполнения дальнейшей привязки этой информации к данным из перехваченных объектов.
4) **Подсистема хранения** должна включать в себя следующие модули:
   - **Модуль хранения настроек системы**, обеспечивающий хранение данных, используемых при обработке и анализе объектов, а также в ходе установки политик и их применения;
   - **Модуль хранения объектов,** обеспечивающий хранение информации об обработанных Системой объектах.
5) **Подсистема Консоль управления** должна обеспечивать управление всеми подсистемами, предоставлять доступ к перехваченной информации и формировать отчёты.
6) **Подсистема визуальной аналитики информационных потоков** должна обеспечивать возможность представления информации из БД Системы в виде интерактивных виджетов и графов связей.
7) **Подсистемы проведения расследований инцидентов ИБ** предназначена для мониторинга групп пользователей с целью локального проведения расследования инцидентов ИБ; анализа рабочей активности и построения картины рабочего дня.

4.1.2. Требования к способам и средствам связи для информационного обмена

Внедряемая Система должна функционировать в составе информационно-вычислительной сети Заказчика.

Система должна корректно работать в сетях доменного типа.

Для информационного обмена между компонентами Системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP.

Система должна поддерживать работу в сетях, работающих по протоколам IPv4 и IPv6.

Должна быть возможность использовать Систему в структуре филиалов, соединенных любыми каналами связи, в том числе с низкой пропускной способностью.

Для информационного обмена между Системой и корпоративной почтовой системой должен использоваться протокол SMTP.

4.1.3. Требования к характеристикам взаимосвязей

Предусмотреть взаимодействие доменов и поддоменов, как связанных, так и не связанных отношениями доверия.

Предусмотреть взаимодействие корпоративных почтовых серверов Заказчика с Системой через механизмы ретрансляции почтового трафика SMTP-relay.

Система должна обеспечивать возможность интеграции и идентификации объектов с данными, полученными из Active Directory, в том числе из нескольких LDAP доменов.

4.1.4. Требования к режимам функционирования Системы

Система должна функционировать в автоматизированном режиме 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.

4.1.5. Требования по диагностированию Системы

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.

4.1.6. Требования к численности и квалификации персонала Исполнителя

Для обеспечения поставки программного комплекса и запуска рабочего функционирования Системы в составе персонала Исполнителя должна присутствовать минимум одна штатная единица инженера технической поддержки.

Инженер технической поддержки должен обладать знаниями в объеме, необходимом для выполнения штатного технического и аварийного обслуживания Системы у Заказчика.

4.1.7. Перспективы развития и модернизации Системы

Система должна быть реализована как открытая система и допускать наращивание производительности за счет улучшения характеристик технических средств.

Система должна обеспечивать возможность модернизации путем замены технического и/или программного обеспечения.

4.1.8. Требования к характеристикам, при которых сохраняется целевое назначение Системы

Система должна обеспечивать штатное функционирование в случае одновременной работы всех пользователей Заказчика на объекте автоматизации.

Целевое назначение Системы должно сохраняться на протяжении всего срока эксплуатации системы. Срок эксплуатации системы определяется сроком устойчивой работы технических средств вычислительных комплексов, своевременным проведением работ по замене (обновлению) технических средств, по сопровождению и обновлению программного обеспечения системы (в рамках гарантийного и послегарантийного обслуживания) и его модернизации.

4.1.9. Требования к унификации

Система должна иметь сертификат ФСТЭК (НДВ4, ТУ).

Сведения о Системе должны быть включены в единый реестр российских программ для электронных вычислительных машин и баз данных.

4.1.10. Требования к надежности

На всех серверах Системы должно быть предусмотрено наличие массива RAID1 (зеркалирование).

Должна быть обеспечена непрерывность бизнес-процессов Заказчика в случае отказов Системы.

При соблюдении штатных условий функционирования, Система обеспечивает работоспособность 24 часа в сутки, 7 дней в неделю, 365 дней в году за исключением технологических окон, определяемых администратором Системы для произведения обновления Системы.

В случае возникновения сбоя технического или программного обеспечения Системы должна быть обеспечена возможность восстановления ее данных и настроек.

Процедуры восстановления работоспособности Системы должны быть описаны и задокументированы в соответствующей эксплуатационной документации на Систему.

4.2. Общие требования к функциям (задачам)

4.2.1. Требования к подсистеме перехвата трафика

Подсистема перехвата трафика должна обеспечивать перехват и обработку трафика, сканирование локальных дисков рабочих станций MS Windows, сетевых разделяемых ресурсов по протоколу SMB, хранилища MS SharePoint, и передачу на обработку объектов или их копий.

Подсистема перехвата трафика должна извлекать из перехваченных объектов текстовую информацию и вложения, выполнять определение форматов вложений и передачу извлеченных данных в подсистему анализа.

Подсистема должна предоставлять возможности обработки следующих типов объектов:

- детектирование форматов изображения (tiff, jpeg, gif, png, bmp, pbm, pgm, ppm, wmf), аудиофайлов (wma, flac, ogg, m4a, aac, ape, mp3, wav), видеофайлы (avi, mpg, wmv, mp4), MS Project (mpp), DjVu (djv, djvu), Adobe Photoshop (psd), Corel Draw (cdr), AutoCAD R14-2013 чертежей и шаблонов (dwg, dwt, dws), DXF (Drawing eXchange Format), Microsoft Publisher (pub), Scalable Vector Graphics (svg), библиотек Linux (so), пакетов linux (rpm), OpenDocument Graphics (odg), файлов баз данных (bmp, bak, trn, full, vcs, vcard, ace mdb, mxl), исполняемых файлов (exe), библиотек Microsoft Windows (dll), документов (chm);
- распаковка архивов gzip, bzip2, tar, arj, zip, rar, lzh, zlib, 7z, а также самораспаковывающихся архивов;
- детектирование и извлечение текста из документов MS Office (doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, vsd), шаблонов MS Office (dot, dotx, dotm, xlt, xltx, xltm, pot, potx, potm), сообщений MS Outlook, документов rtf, xps, html, Windows icon (ico), изображений emf.

Подсистема должна поддерживать кодировки: iso-8859-1, iso-8859-15, iso-8859-5, Windows-1251, Windows-1252, koi8-r, utf-8, utf-16.

4.2.1.1. Требования к модулю контроля корпоративной почты

Модуль должен предоставлять возможности для контроля сообщений и вложений, переданных по протоколам SMTP, POP3, IMAP, MAPI помощи любых почтовых клиентов.

Модуль контроля корпоративной почты должен обеспечивать возможность осуществлять разрешение или блокировку для пользователей на отправку почтовых сообщений. Блокировка почтовых отправлений осуществляется по протоколам SMTP (MAPI) и IMAP по результатам анализа переданного текста и вложений.

Модуль должен расшифровывать сообщения, сформированные по стандарту S/MIME, если сообщения переданы с помощью Outlook (MAPI) и используется криптографический провайдер Microsoft.

Модуль должен выполнять выделение транспортных атрибутов (отправитель, список получателей) из перехваченных данных.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

4.2.1.2. Требования к модулю контроля web-трафика

Модуль контроля Web-трафика должен обеспечивать получение данных копии HTTP(S)-трафика, полученного как с рабочей станции, так с прокси-сервера по протоколу ICAP, и подготовку этих данных к дальнейшему анализу.

Модуль контроля Web-трафика должен обеспечивать перехват загружаемых данных по протоколам HTTP(S) и по результатам анализа обеспечивать блокировку передачи данных.

Модуль контроля Web-трафика должен обеспечивать получение копии файлов, загруженных на FTP-ресурсы, и подготовку этих данных к дальнейшему анализу.

Модуль контроля Web-трафика должен обеспечивать перехват загружаемых файлов на FTP-ресурсы и по результатам анализа осуществлять блокировку передачи данных.

Модуль должен поддерживать обработку POST- и PUT-запросов (выделение атрибутов отправитель, список получателей, тема сообщения и обработку текста).

Модуль контроля Web-трафика должен обеспечивать возможность осуществлять разрешение или запрет для пользователей на использование FTP-ресурсов.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

4.2.1.3. Требования к модулю контроля программ мгновенного обмена сообщениями

Модуль контроля программ сетевого общения должен обеспечивать перехват и обработку следующих данных:

- сообщений чатов и файлов, отправленных при помощи сервиса обмена мгновенными сообщениями ICQ, Jabber, Skype, Microsoft Lync и приложений, работающих по протоколу XMPP;
- голосовых переговоров в Skype;

Модуль контроля программ сетевого общения должен обеспечивать возможность осуществлять разрешение или запрет для пользователей использования сервисов обмена мгновенными сообщениями: Skype и приложений, работающих по протоколу XMPP.

Модуль должен выполнять выделение транспортных атрибутов (отправитель, получатель) из перехваченных данных.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

4.2.1.4. Требования к модулю контроля съемных носителей, приложений на рабочей станции

Модуль должен обеспечивать возможность осуществлять разрешение или запрет для пользователей работы с периферийными устройствами, в том числе ограничивать доступ только на чтение.

Модуль должен обеспечивать возможность разрешения или запрета для пользователей:

- работы с облачными хранилищами (DropBox, Google Drive, Яндекс.Диск, Microsoft OneDrive, Evernote, SugarSync);
- работы с приложениями на рабочих станциях, а так же использования буфера обмена и печати в приложениях;
- контроль доступа терминальных клиентов подключенных к терминальному серверу посредством Microsoft RDP или Citrix ICA;
- контроль снимков экрана на рабочих станциях.

Модуль должен обеспечивать перехват и обработку следующих данных:

- теневых копий файлов при копировании информации на съемные носители;
- файлов при редактировании непосредственно на съемных устройствах;

Модуль должен обеспечивать перехват теневых копий только с устройств, которые определяются в качестве съемных устройств хранения.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

Модуль должен обеспечивать возможность перехвата загружаемых файлов на съемные устройства и по результатам анализа осуществлять блокировку передачи данных.

4.2.1.5. Требования к модулю контроля печати документов

Модуль контроля печати документов должен обеспечивать возможность осуществлять разрешение или запрет для пользователей работы с принтерами.

Модуль контроля печати документов должен обеспечивать перехват и обработку теневых копий файлов, отправленных на печать на локальные и сетевые принтеры.

Модуль должен обеспечивать возможность запрета печати документов из сформированного списка приложений на локальные, сетевые и терминальные принтеры.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

4.2.1.6. Требования к модулю аудита хранения информации

Модуль аудита хранения информации должен обеспечивать сканирование файлов локальных дисков рабочих станций под управлением MS Windows, сетевых разделяемых ресурсов. файлового хранилища MS SharePoint, подготовку этих данных к дальнейшему анализу и передачу их в модуль обработки теневых копий.

В качестве параметров поиска могут выступать следующие атрибуты:

- Рабочие станции, группы Active Directory;
- Размеры файлов;
- Типы файлов;
- Контекстный поиск;

4.2.1.7. Требования к модулю контроля мобильных устройств

Модуль должен осуществлять перехват и анализ изображений, снятых с помощью камеры мобильного устройства, создание теневых копий SMS-сообщений, а также сообщений и файлов, отправленных с использованием систем мгновенного обмена сообщениями WhatsApp и Skype, для устройств под управлением операционной системой iOS.

Модуль должен осуществлять перехват и анализ изображений, снятых с помощью камеры мобильного устройства, создание теневых копий SMS-сообщений, а также сообщений и файлов, отправленных с использованием систем мгновенного обмена сообщениями WhatsApp и Skype, с использованием почтовых клиентов и web-браузера, для устройств под управлением операционной системой Android.

Модуль также должен осуществлять контроль запуска приложений на мобильном устройстве.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

4.2.1.8. Требования к модулю создания снимков экрана

Модуль должен обеспечивать создание снимков экрана с рабочих станций пользователей и обеспечивать их передачу в подсистему хранения.

Модуль должен обеспечивать возможность просмотра имеющихся снимков экрана через web-консоль.

4.2.2. Требования к подсистеме анализа

Подсистема анализа должна обеспечивать анализ текстовых данных, извлеченных из перехваченных объектов (тексты писем, сообщений, запросов, а также тексты, извлеченные из вложений), анализ наличия в перехваченных объектах выгрузок из баз данных, анализ наличия изображений главного второго разворота паспорта гражданина РФ, изображений кредитных карт, изображений топографических карт, чертежей и официальных печатей.

Подсистема анализа должна обеспечивать анализ бинарных данных, присутствующих в перехваченных объектах. Бинарные данные должны анализироваться подсистемой в том случае, когда извлечение текста не возможно или помимо текста в передаваемом документе присутствует информация другого рода (изображения, музыка и т.д.).

Подсистема анализа должна передавать все данные, полученные в результате анализа перехваченных объектов, в подсистему применения политик.

4.2.2.1. Требования к модулю OCR

Модуль OCR – должен обеспечивать распознавание текста, содержащегося в изображениях, полученных от подсистемы перехвата трафика и теневых копий.

Модуль должен обеспечивать передачу перехваченных объектов подсистеме анализа.

4.2.2.2. Требования к модулю лингвистического анализа

Модуль лингвистического анализа должен обеспечивать классификацию текста объекта путем поиска соответствия этого текста каким-либо категориям.

Система должна выполнять лингвистический анализ с использованием лингвистических алгоритмов, основанных на поиске определенных терминов (слов и словосочетаний) образующих иерархический справочник категорий, причем извлеченный текст может содержать опечатки или транслитерацию.

Система должна предоставлять возможность настройки алгоритма лингвистического анализа посредством графического пользовательского интерфейса: задавать иерархию справочника категорий, задавать термины и их значимость, учитывать морфологию, используемый регистр символов.

Система должна предоставлять возможность проведения лингвистического анализа для русского и английского языка.

В Системе должен быть преднастроенный стандартный классификатор, содержащий категории «Грифы секретности» и «Структура компании», а также отраслевой классификатор «Энергетика»

4.2.2.3. Требования к модулю детектирования цифровых отпечатков

Система должна выполнять поиск фрагментов, принадлежащих к задаваемым эталонным документам, составляющим базу эталонных документов.

Для добавляемых пользователем эталонных документов должен формироваться текстовый, бинарный или текстовый и бинарный отпечатки. Если для загруженного документа Системой невозможно извлечь текстовую информацию, должен формироваться только бинарный отпечаток эталонного документа.

Для бинарных и для текстовых данных должна поддерживаться возможность указания порога цитируемости.

4.2.2.4. Требования к модулю детектирования текстовых объектов

Модуль детектирования текстовых объектов должен выполнять поиск тестовых объектов, соответствующих регулярным выражениям, в соответствии с предустановленными шаблонами.

Модуль должен обеспечивать возможность указания страны принадлежности каждого текстового объекта.

4.2.2.5. Требования к модулю детектирования графических объектов

Модуль детектирования графических объектов должен позволять отслеживать наличие в поступающих на анализ изображений топографических карт, чертежей и прочих графических объектов.

Должна обеспечиваться поддержка графических объектов в виде растровой графики, векторной графика, чертежей, выполненных на белом фоне и 3D описания моделей PLM систем.

4.2.2.6. Требования к модулю детектирования кредитных карт

Модуль детектирования графических объектов должен позволять отслеживать наличие в поступающих на анализ изображениях кредитных карт.

Для детектирования кредитных карт не должно требоваться добавление эталонных документов в Систему.

4.2.2.7. Требования к модулю детектирования паспортов

Модуль детектирования паспортов должен позволять отслеживать наличие в поступающих на анализ изображениях второго главного разворота паспорта гражданина Российской Федерации.

Для детектирования паспортов не должно требоваться добавление эталонных документов в Систему.

4.2.2.8. Требования к модулю детектирования выгрузок из баз данных

Модуль должен обеспечивать детектирование в текстах и вложениях объектов выгрузок из баз данных.

Модуль должен предоставлять возможность задания следующих условий детектирования выгрузок из баз данных:

1. Условия совокупности столбцов, сочетание которых будет считаться конфиденциальной информацией (например, только ФИО сотрудника не будет являться таковой, а ФИО сотрудника с контактным телефоном и номером и серией паспорта будет);
2. Задание количества строк, обнаружение которых будет детектироваться как наличие в объекте выгрузки из баз данных.

В перехваченных объектах должна присутствовать информация о детектировании выгрузки из БД.

4.2.2.9. Требования к модулю детектирования печатей

Модуль детектирования печатей должен позволять отслеживать наличие эталонных печатей на изображениях отсканированных документов.

В информации о перехваченных объектах, в которых детектировалось присутствие эталонных печатей, должно содержаться имя файла эталона и данные о релевантности эталона по отношению к захваченному изображению.

4.2.3. Требования к подсистеме применения политик

Подсистема применения политик должна, на основе результатов работы подсистемы анализа и подсистемы обработки, выполнять вынесение вердикта о факте нарушения или не нарушения перехваченным объектом политики информационной безопасности. Подсистема

должна обеспечивать привязку данных о получателе или отправителе объекта к записям справочника сотрудников и рабочих станций.

Подсистема должна устанавливать соответствие перехваченных и проанализированных объектов, персонам, рабочим станциям и группам, полученным из Active Directory или созданным пользователем в Системе.

Идентификация сотрудника должна осуществляться по адресу электронной почты, Web-контакту, IP-адресу рабочей станции, логину Skype, логину ICQ, или по авторизационной информации (логин, домен) отправителя.

Объектам, полученным в результате сканирования модулем аудита хранения информации, информация об отправителе и получателе должна присваиваться по следующему принципу:

- Отправитель – владелец файла;
- Получатели – список пользователей, имеющих доступ к файлу не ниже уровня «чтение».

Идентификация рабочей станции должна осуществляться по IP-адресу и DNS имени рабочей станции.

При идентификации перехваченных объектов, прошедших процедуру разбора, должно осуществляться сравнение идентификационной информации, содержащейся в служебных атрибутах, с идентификационной информацией, полученной из Active Directory или заданной пользователем Системы.

4.2.3.1. Требования к модулю интеграции с Active Directory

Модуль интеграции с Active Directory должен обеспечивать возможность первоначального импорта и периодической синхронизации структуры каталога Active Directory со справочником сотрудников и рабочих станций для выполнения дальнейшей привязки этой информации к данным из перехваченных объектов.

Система должна предоставлять возможность настройки периода сканирования измененных элементов. При сканировании измененных элементов в Системе учитываются только последние изменения, произошедшие с момента последнего сканирования изменений.

Система должна предоставлять возможность настройки периода и времени сканирования Active Directory.

Модуль интеграции с Active Directory должен передавать все данные, полученные в результате импорта или синхронизации, в подсистему хранения.

4.2.3.2. Требования к модулю принятия решений

Модуль принятия решений должен обеспечивать применение политики информационной безопасности путем выполнения для объектов правил из сценария обработки объектов.

Модуль должен предоставлять возможности для задания правил автоматического вынесения вердикта по объекту. Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:

- атрибутов перехваченного объекта;
- логического периметра;
- результатов лингвистического анализа текста, извлеченного из перехваченного объекта;
- результатов анализа технологии детектирования цифровых отпечатков;
- результатов анализа технологии детектирования графических объектов;
- результатов анализа технологии детектирования кредитных карт;
- результатов анализа технологии детектирования паспортов;
- результатов анализа технологии детектирования эталонных выгрузок из БД;
- результатов анализа технологии детектирования эталонных печатей;
- результатов анализа технологии детектирования текстовых объектов;
- результатов идентификации отправителя перехваченного объекта.

Модуль должен предоставлять возможности для автоматического проставления перехваченным объектам дополнительных атрибутов (теги, цвет), отображаемых в пользовательском интерфейсе Системы.

Для объектов с вложениями модуль должен присваивать объекту тег, соответствующий типу файла вложения.

Для HTTP- и HTTPS-запросов модуль должен определять тип сайта, на который направлен запрос, и присваивать объекту тег, соответствующий типу сайта.

Модуль должен предоставлять возможности для передачи объектов в подсистему хранения.

4.2.4. Требования к подсистеме хранения

Подсистема должна обеспечивать хранение информации о перехваченных объектах, результатах их анализа и применения политик, а также предоставлять возможность для просмотра хранящейся информации посредством запросов из консоли управления.

Подсистема хранения должна предоставлять возможность хранить часть данных на «быстрых» дисках. При использовании данной возможности значительно уменьшается время выполнения поисковых запросов при работе в Консоли управления.

Подсистема должна обеспечивать возможность устанавливать различный период хранения, как для всех объектов, так и только для объектов с нарушениями.

4.2.4.1. Требования к модулю хранения настроек системы

Модуль хранения настроек системы должен обеспечивать хранение данных, используемых при обработке и анализе объектов, а также в ходе установления политик и их применения:

- актуальные данные о структуре Active Directory, рабочих станциях и учетных записях сотрудников.
- группы, созданные пользователями в Системе, объединяющие учетные записи сотрудников/рабочих станций. Группы, созданные пользователями в Системе, не могут содержать другие группы в качестве своих элементов;
- информация о настройке уведомлений пользователей о нарушениях и их шаблонах;
- настройки соединения с сервером аудита хранения информации.
- информация о конфигурации Системы и истории ее изменений.

4.2.4.2. Требования к модулю хранения объектов

Модуль хранения объектов должен обеспечивать хранение информации об обработанных Системой объектах:

- данные (атрибуты, текст), извлеченные из объекта, в том числе из вложений, имеющихся у объекта;
- результаты идентификации отправителя и получателей объекта;
- результаты анализа объекта;
- информацию о решении по объекту (вердикту).

С целью освобождения пространства на жестком диске модуль должен позволять архивировать сегменты БД хранилища с последующим размещением на каком-либо носителе информации с возможностью их последующего восстановления.

4.2.5. Требования к подсистеме Консоль управления

Подсистема Консоль управления предоставляет возможности управления настройками Системы, правами пользователей на работу с функциями Системы, настройки подсистемы анализа, подсистемы применения политик, просмотра информации о перехваченных объектах и выполнения ретроспективного анализа этих объектов.

В Консоли управления должна быть предусмотрена возможность по разграничению доступа пользователей к перехваченным объектам (автоматическое отнесение перехваченного объекта к той или иной зоне ответственности на основании правил).

В Консоли управления должна быть предусмотрена возможность проводить полный аудит действий офицера безопасности в консоли системы.

В Консоли управления должна быть предусмотрена возможность для управления зонами ответственности пользователей системы (в том числе для настройки маршрутов перемещения объектов между зонами ответственности).

В Консоли управления должна быть предусмотрена возможность получения детализированных отчетов в интерактивном режиме.

В Консоли управления должна быть предусмотрена возможность проводить полноценный текстовый поиск по всем событиям или только по вложениям.

В Консоли управления должна быть предусмотрена возможность для подготовки статистических отчетов по перехваченным объектам в следующих форматах: pdf и html.

4.2.6. Требования к подсистеме визуальной аналитики информационных потоков

Подсистема должна являться инструментом визуальной аналитики информационных потоков корпоративной сети Заказчика в режиме реального времени.

Подсистема автоматизирует следующий вид деятельности Заказчика:

- Выявление подозрительной активности и связей сотрудников, которые остаются вне поля зрения политик Системы
- Обеспечение мгновенного доступа к деталям любой подозрительной активности;
- Предоставление гибкой отчетности в режиме реального времени для любого среза данных.

Подсистема должна обрабатывать информацию из базы данных Системы и далее предоставлять доступ к этой информации в режиме реального времени Системы защиты конфиденциальной информации.

Подсистема должна обеспечивать:

- построение интерактивного графа связи для анализа связи сотрудников компании, внешних контактов и перемещение информации на USB-накопители, принтеры и веб-ресурсы. Узлы и связи на графе должны быть интерактивными – с возможностью посмотреть детализацию по событиям и сотрудникам;
- формирование интерактивного досье на сотрудника компании или любого внешнего контакта с отображением детализации по событиям, а также построение индивидуального графа связи;
- формирование динамической сводки безопасности по всей компании или по отделам с возможностью перестраивать сводку по новым срезам данных в режиме реального времени;
- предоставление конструктора для построения специфических отчётов по инцидентам информационной безопасности с возможностью выгружать результаты в формате PDF и PPT.

4.2.7. Требования к подсистеме проведения расследований инцидентов ИБ

Подсистема должна являться средством мониторинга групп пользователей с целью локального проведения расследования инцидентов ИБ; анализа рабочей активности и построения картины рабочего дня.

Подсистема должна обеспечивать:

- перехват информации с устройства аудио/видеозаписи, устройства ввода текста, буфера обмена; анализа динамики, скорости ввода текста, частоты возникновения ошибок; сбора статистики по контактам с отображением граф-связей.
- перехват и записи голосовых переговоров в Skype, Lync, Viber.
- мониторинг и отображение отчетов по активности пользователя в течение заданного периода: мониторинг программ и сайтов, поисковых запросов, файловых операций.
- мониторинг устанавливаемого ПО и изменений в составе оборудования для рабочего места.
- предоставление возможности администратору и офицеру безопасности в онлайн режиме: отправки текстовых сообщений пользователю; получать доступ к изображению рабочего стола пользователя, веб-камере, устройству записи голоса.
- для устройств на базе Android осуществлять перехват голосовых разговоров, GPS данных с построением визуального маршрута.

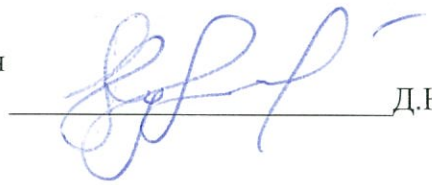
5. Требования по вводу в действие программного обеспечения Системы

Ввод в действие программного обеспечения системы предотвращения утечек конфиденциальной информации должен включать комплекс работ по установке программных компонент с последующей их настройкой в соответствии с положениями документации, разработанной в ходе первого этапа (консультационные услуги).

6. Требования к параметрам и составу услуг по технической поддержке Системы

- Часовое покрытие - 14x5 по рабочим дням с 07:00 до 21:00 (время московское)
- Первичный ответ – в течение 8 часов
- Поддержка по электронной почте
- Поддержка по телефону

- Удаленное подключение для решения проблем
- Выезд к заказчику для решения проблем на месте
- Доступ к базе знаний
- Бесплатное исправление критических ошибок (патчи) ошибок
- Бесплатное плановое обновление (сервисные релизы)
- Бесплатное обновление до новой версии
- Вебинары по продуктам и сервисам
- Профилактика (выезд к клиенту, сбор информации, проактивное решение возможных проблем) 1 раз в год

Начальник службы системно-технического обеспечения  Д.Ю. Куликов