«УТВЕРЖДАЮ»
Заместитель Председателя Правления
АКБ «Банк Развития Бизнеса»
_____ и.о. О.Р.Вохидов
«____»_____2024 г.

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ
«Программное обеспечение для защиты информации»

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 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.

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. Клиентская часть Системы, осуществляющая контроль процесса передачи конфиденциальной информации на уровне рабочих станций пользователей, должна быть представлена программным Агентом.

1.3. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Windows: Windows 8, 8.1 x32/x64, Windows 10 x32/x64, Windows 11 x64, Windows Server 2016, Windows Server 2019, Windows Server 2022.

1.4. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Linux: Alt Linux 8 СП x64, 9 x64, 10 x64; Astra Linux 1.6 x64 («Смоленск»), 2.12 x64 («Орёл»), Special Edition 1.7 x64; CentOS 8 x64; RedOS 7.3 x64; Ubuntu 20.04 x64, 22.04 x64, 24.04 x64.

1.5. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства MacOS: Monterey 12.1, Ventura 13.3, Sonoma 14.0, Sequoia 15.0.

1.6. 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. Требования к функциям Агента для ОС Windows представлены в п. 5.3.1, требования к функциям Агента для ОС Linux представлены в п. 5.3.2, требования к функциям Агента для ОС MacOS представлены в п. 5.3.3.

1.7. Все серверные функции Системы должны выполняться в рамках единого решения, единой СУБД для архивирования данных и работать в рамках одной линейки ОС. Исключением служат сторонние сервисы, с которыми Система имеет возможность интеграции.

1.8. Система должна поддерживать работу в замкнутом контуре, то есть в локальной сети Заказчика без выхода в сеть Интернет. Исключением служат отдельные опциональные функции, выключенные по умолчанию и активируемые только по желанию Заказчика (такие как передача данных агентами через Интернет, подключение к облачным корпоративным сервисам и другие функции, в явном виде требующие интернет-соединения).

1.9. Все сетевые соединения, протоколы связи и направления соединений должны быть указаны в технической документации на Систему.

1.10. Система должна обеспечивать защиту данных, передаваемых агентскими или клиентскими компонентами по линиям связи.

1.11. Система мониторинга, анализа и визуализации внутреннего трафика (Далее – Система мониторинга) должна предоставляться в виде виртуального программного обеспечения и функционировать в режиме постоянной лицензии с поддержкой сроком на 3 года.

2. Требования к поставке лицензионных программных средств

2.1. 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.

2.2. Исполнитель должен предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие права на обновление и поддержку (гарантийное сопровождение) программного обеспечения в течение 36 (тридцати шести) месяцев.

2.3. Подсистемы контентного анализа и принятия решений должны лицензироваться за единицы (одна лицензия на каждую подсистему).

2.4. Модули подсистемы контроля должны иметь лицензирование по конечным пользователям: это значит, что одна лицензия требуется для одной подконтрольной (защищаемой Системой) доменной или локальной учетной записи. Исключением служит модуль аудита файлов, где лицензирование происходит по количеству рабочих станций (в случае использования Агента Системы на клиентских версиях (workstation) операционных систем) или по объему сканируемых данных (в случае сетевого сканирования или использования Агента на серверных версиях (server) операционных систем).

2.5. Лицензии модулей подсистемы контроля должны быть конкурентными. Это значит, что одну лицензию можно использовать для контроля разных пользователей (учетных записей) / рабочих станций только в разные периоды времени.

3. Программное обеспечение должно включать следующие модули и подсистемы:

№	Наименование
1.	Подсистема контроля, состоящая из:
1.1.	модуль контроля электронной почты
1.2.	модуль контроля сервисов обмена мгновенными сообщениями
1.3.	модуль контроля FTP-соединений
1.4.	модуль контроля HTTP-трафика (POST- и GET-запросы)
1.5.	модуль контроля печати
1.6.	модуль контроля и управления доступом съёмных устройств
1.7.	модуль контроля событий на мониторах и действий сотрудников
1.8.	модуль контроля разговоров сотрудников
1.9.	модуль контроля активности пользователей и приложений
1.10.	модуль контроля облачных хранилищ данных
1.11.	модуль аудита файлов
2.	Подсистема контентного анализа
3.	Подсистема принятия решений
4.	Система сбора, долгосрочного хранения, анализа и визуализации конфигураций, журналов, настроек и других параметров сервисов серверной и сетевой инфраструктуры, мониторинга журналов и анализа событий

4.1. Количество лицензий

№	Наименование лицензии	Количество, шт.
1.	Лицензия на DLP	1000 рабочих станций
2.	Модуль DLP для аудита файлов АРМ	1000 рабочих станций
3.	Модуль DLP для аудита файлов на сервере (в ТБ)	10 ТБ сетевого хранилища файлов
4.	Обрабатываемые системой мониторинга события в секунду (EPS)	5000

Тип лицензирования – бессрочные лицензии.
Гарантийная поддержка разработчика/правообладателя на весь программный комплекс – 3 календарных года с даты подписания акта передачи лицензий.

4. Технические требования к Системе

4.1. Требования к Системе в целом

Система должна поддерживать контроль и защиту передачи конфиденциальной информации в рамках каналов, описанных в настоящем техническом задании, а также ее автоматизированный анализ в рамках технологий, указанных в настоящем техническом задании.

Система должна предполагать возможность выборочной активации модулей контроля для вышеперечисленных каналов передачи данных.

Система должна обеспечивать разграничение прав доступа к архиву информации, политикам безопасности и настройкам Системы.

Система должна иметь удобный и понятный пользовательский интерфейс, где все сообщения и документация должны быть на русском языке.

Пользователь Системы должен иметь выбор между «толстым» клиентом и веб-интерфейсом при работе с результирующими отчетами Системы, при этом разграничение доступа должно быть централизованным и индивидуальным как при работе в «толстом» клиенте, так и в веб-интерфейсе.

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.

Система должна обеспечивать контроль почтового трафика как на уровне рабочих станций, так и на уровне интеграции с корпоративным почтовым сервером.

Система должна обладать возможностью оптимизации нагрузки на ресурсы территориально разделенных сетей с «узким» каналом передачи данных благодаря предварительному сжатию информации, настройке расписания, маршрутов передачи и ограничения скорости передачи, а также за счет возможности задействовать промежуточные серверы обработки и временного хранения данных.

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.

Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах ОС Windows для всех указанных в п.1.3 операционных систем.

Агент Системы, осуществляющий контроль на уровне рабочих станций с ОС Windows, должен быть подписан цифровой подписью.

Подсистема контентного анализа должна предоставлять возможности:

- проведения ретроспективного анализа архива информации, учитывая возможность изменения правил проверки;
- генерации отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности;
- просмотра активности пользователей в режиме реального времени.

Подсистема принятия решений должна предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту – нарушает или не нарушает он существующие правила.

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.

Модуль контроля сервисов обмена мгновенными сообщениями должен обеспечивать контроль сообщений и файлов, переданных при помощи популярных интернет-мессенджеров. В

частности, обеспечивать контроль сеансов текстовой и голосовой связи, файлов и SMS-сообщений, переданных посредством Skype, контроль чатов, звонков и файлов коммуникационных клиентов Microsoft Lync, Viber Desktop, Telegram Desktop и Zoom Chat.

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).

Модуль контроля HTTP-трафика должен обеспечивать контроль POST- и GET-запросов при использовании пользователями Заказчика интернет-сервисов, а также иметь подключаемую функцию автоматической остановки трафика в случае возникновения инцидента, зарегистрированного данным модулем.

Модуль контроля печати должен обеспечивать контроль документов, отправленных на печать при помощи сетевых или локальных принтеров.

Модуль контроля и управления доступом съемных устройств должен обеспечивать контроль файлов, записываемых на USB-устройства, CD-/DVD-матрицы и др. типы съемных устройств.

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. Техническая возможность и методика реализации в данном случае определяется Разработчиком Системы.

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.

Модуль контроля активности пользователей и приложений должен обеспечивать мониторинг активности пользователей и запускаемых ими процессов с учетом длительности в течение рабочего дня.

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, RealVNC, Radmin, LiteManager).

Модуль аудита файлов должен обеспечивать аудит всех файловых операций, обеспечивать сканирование содержимого файлов в локальных и сетевых файловых системах в соответствии с настроенными правилами сканирования, производить индексацию файлов рабочей станции, сохранять древовидную копию структуры файловой системы, производить аудит прав доступа к объектам файловой системы.

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.

Система мониторинга должна обеспечивать обработку не менее 85000 Flow в секунду.

Система мониторинга должна, вне зависимости от наличия ресурсов, обрабатывать все приходящие к ней события. Не должно быть блокировок программных функций при временном превышении количества событий.

Система мониторинга должна предоставлять возможность визуализации собранных данных с сетевого потока, а также настройку кастомных пользовательских панелей мониторинга.

Система мониторинга должна мониторить и анализировать трафик на уровне приложений для выявления и устранения проблем с производительностью приложений.

Система мониторинга должна обеспечивать предоставление детализированных отчетов о трафике в реальном времени с возможностью просмотра статистики и анализа динамики трафика.

Система мониторинга должна иметь возможность сохранения и архивирования исторических данных для последующего анализа и составления отчетов.

Система мониторинга должна иметь возможность интеграции с существующими сетевыми устройствами для сбора данных без дополнительных сложностей.

Система мониторинга должна поддерживать возможность уведомления о событиях с использованием алертов и предоставлять выбор различных средств для уведомлений, включая Email, Telegram, Jira, Microsoft Teams, Google Chat и другие.

Система мониторинга должна иметь возможность применения пользовательских фильтров и правил для настройки процесса мониторинга и анализа в соответствии с потребностями организации.

Система мониторинга должна обладать гибкостью масштабирования для обработки больших сетей и объемов трафика.

Система мониторинга должна поддерживать работу в распределенном режиме для обеспечения отказоустойчивости и непрерывной доступности мониторинга и анализа.

Система мониторинга должна иметь поддержку различных форматов журналов и возможность экспорта данных.

Система мониторинга должна иметь возможность определения аномалий и атак в сетевом трафике, а также предоставление средств для реагирования на них.

В системе мониторинга должна быть предусмотрена возможность фильтрации данных, отображаемых на информационных панелях. Фильтрация должна выполняться в соответствии с интуитивными критериями, и должна быть возможность комбинировать несколько критериев с помощью стандартных логических операторов И/ИЛИ/НЕ (AND/OR/NOT). Решение не должно использовать специализированный синтаксис для реализации данного требования.

Система мониторинга должна обеспечивать возможность экспорта отчетов по индивидуально настраиваемым расписаниям и временным интервалам их выполнения. Отчеты должны быть настроены оператором системы и должны либо храниться на устройстве, либо отправляться на ранее назначенные адреса электронной почты или отправляться на ранее указанный сетевой ресурс.

Система мониторинга должна иметь возможность создавать графики на основе событий. Вершины графов должны иметь размер в зависимости от количества связанных с ними событий.

4.2. Требования к способам и средствам связи для информационного обмена

Система должна функционировать в составе информационно-вычислительной сети Заказчика.

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.

Система должна корректно работать в сетях доменного типа.

Система должна поддерживать работу в виртуальной инфраструктуре. Перечень сред виртуализации, прикладного ПО и его версий, поддерживаемых Системой, должен передаваться Исполнителем в составе технической документации.

Для информационного обмена между компонентами Системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet) и\или беспроводные сетевые соединения.

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

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).

Система мониторинга должна быть способна эффективно обрабатывать не менее 100 ГБ данных в день.

Система мониторинга, анализа и визулазации внутреннего трафика так же должна собирать данные следующими методами: пассивный сбор журналов (SYSLOG), сбор журналов с аутентификацией (CIFS или более новая реализация, совместимая со всеми поддерживаемыми в настоящее время системами Microsoft Windows, SCP), CEF, OPSEC, SDEE, XML, ODBC. или JDBC.

Система мониторинга должна иметь возможность переопределять поле географического местоположения для событий с внутренними (частными) IP-адресами в соответствии с настроенной схемой.

Система мониторинга должна быть подключена к репутационной базе данных IP-адресов, идентифицированных как части ботнетов, сетей TOR и других базах скомпрометированных IP-адресов.

Система мониторинга должна обеспечивать возможность мониторинга задержки, нагрузки на интерфейсах подключаемых источников сетевого трафика.

Система мониторинга должна иметь не менее 800 встроенных предопределенных правил корреляции, готовых к использованию сразу после подключения источников данных.

Система мониторинга должна уметь синхронизировать время по протоколу NTP.

Связь между устройствами системы мониторинга, расположенными в разных местах, и связь с конечным пользователем должны быть зашифрованы как минимум с использованием криптографического алгоритма AES-256 или эквивалентного или с более высокими параметрами безопасности.

Система мониторинга должна поддерживать сетевые потоки в различных форматах, включая v5, v9, jflow и sflow, для обеспечения совместимости с разными устройствами и протоколами.

Решение должно обеспечивать полную поддержку стандарта IPv6 (управление, сбор событий и сетевых потоков).

4.3. Требования к режимам функционирования Системы

Система должна обеспечивать возможность работы в следующих режимах:

- штатный режим (основной режим функционирования, предусматривающий автоматизированную работу Системы под управлением администратора, при которой обеспечивается непрерывное круглосуточное выполнение всех функций Системы);
- сервисный режим (используется для проведения обслуживания, реконфигурации и модернизации компонентов);
- автономный режим (используется в случае отсутствия связи между компонентами Системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

4.4. 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.

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.

В случае многопользовательской работы модуль должен автоматически создавать раздельные журналы для каждого пользователя.

4.5. Требования к численности и квалификации персонала Исполнителя

Для обеспечения поставки и ввода в эксплуатацию 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.

4.6. Перспективы развития и модернизации Системы

Система должна допускать наращивание производительности за счет улучшения характеристик технических средств.

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

Исполнитель может привлекаться для консультаций Заказчика для согласования минимально достаточного или рекомендуемого оборудования при планировании внедрения Системы. Консультации должны носить формализованный вид и быть построены на базе типового анкетирования Заказчика.

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

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.

Целевое назначение Системы должно сохраняться на протяжении всего срока эксплуатации Системы для заранее оговоренного ИТ-окружения. Поддержка новых версий системного или прикладного ПО, не оговоренных отдельно с Исполнителем и вышедших в будущем не может быть гарантирована.

4.8. Требования к функциям администрирования

Интерфейс администратора должен предоставлять возможность контроля работоспособности Системы.

Интерфейс администратора должен предоставлять возможность отображения статистики работы Агентов, серверных подсистем перехвата данных с рабочих станций, сервера индексации, служб контроля почтовой переписки (на уровне интеграции с корпоративным почтовым сервером), службы блокировки почты, СУБД MS SQL Server и PostgreSQL, служб распознавания графических изображений и аудиофайлов, операционной системы. Для всех указанных статистических данных должна быть реализована возможность обеспечения резервного копирования.

Интерфейс администратора должен обеспечивать возможность управления службами подсистем.

Интерфейс администратора должен предоставлять возможность управления базами данных модулей контроля информации.

Интерфейс администратора должен предоставлять возможность мониторинга дискового пространства на серверах Системы.

Интерфейс администратора должен предоставлять возможность автоматического оповещения о важных событиях (сбои в работе, нехватка свободного места, превышение количества лицензий и другие).

Интерфейс администратора должен обеспечивать возможность синхронизации с одним или более доменом Active Directory.

Интерфейс администратора должен обеспечивать возможность работы с пользователями рабочих групп.

Интерфейс администратора должен предоставлять возможность разграничения прав доступа сотрудников службы безопасности к функциям 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.

Интерфейс администратора должен предоставлять возможность указания настроек для подключения к базам данных (для случаев, когда они используются), которые можно впоследствии использовать по умолчанию.

Интерфейс администратора должен обеспечивать возможность управления настройками функций сбора статистики и предоставления отчетов, настройками модуля принятия решения, служб распознавания графических изображений и аудиофайлов, а также обеспечивать возможность настройки просмотра отчетов посредством веб-интерфейса.

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.

Система мониторинга должна обеспечивать возможность разделения ролей и привилегий отдельных пользователей системы, например:

- административный доступ;
- доступ оператора;
- доступ только для чтения;
- доступ к данным, собранным из определенных источников.

Кроме того, пользователь в своей учетной записи должен иметь возможность создавать правила, создавать фильтры и создавать отчеты.

4.9. Требования к хранению данных

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. Техническая возможность определяется Разработчиком Системы.

Система должна иметь опцию хранения текстовой и атрибутивной информации в специализированных индексах для ускорения поисковых выборок. В случае, когда информация содержится в индексе, любой поисковый запрос такой информации также должен сначала выполняться по индексу.

Система должна быть совместима с Microsoft SQL Server 2012 SP4 и выше, а также с PostgreSQL 14 и выше для хранения информации в структурированной табличной форме и дальнейшей ее обработки в сторонних системах анализа.

Система должна архивировать все перехваченные объекты, а не только те, по которым зафиксированы инциденты.

Система мониторинга должна обеспечивать возможность хранения собранной информации на внешних запоминающих устройствах типа DAS или NAS (NFS, CIFS) или SAN (iSCSI, FC).

Записанные данные из системы мониторинга в предоставленной системе хранения данных должны быть доступны для просмотра и анализа оператором непосредственно из консоли системы, без необходимости выполнения дополнительных действий вне консоли. Если данные находятся в

автономном режиме, должна быть возможность загрузить данные в систему, чтобы сделать их доступными в режиме реального времени.

Архивирование данных системы мониторинга должно поддерживать интеграцию с Amazon S3, Azure Blob Storage, NAS и SAN.

4.10. Требования к надежности

На всех серверах Системы должно быть предусмотрено наличие массива RAID.

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.

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.

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

5. Требования к функциям (задачам), выполняемым Системой

5.1. Требования к подсистеме контентного анализа

Подсистема контентного анализа должна быть ориентирована на работу с данными, получаемыми от модулей подсистемы контроля.

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.

Подсистема должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных или запротоколированных объектов, обозначенных в разделе 5.3. По объектам, для которых в Системе настроена индексация данных, должны поддерживаться следующие поисковые возможности:

- поиск, по ключевым словам, и фразам в базах перехваченных документов;
- выборка перехваченных данных по дате, доменному имени пользователя, адресам и хостам электронной почты, псевдонимам Skype, 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.

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.

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, а также соотношения видеозаписи с активностью приложений и нажатиями клавиш.

Подсистема должна предоставлять возможность просмотра контентного маршрута перехваченного документа.

Подсистема должна предоставлять возможности экспорта выборки перехваченных данных (полного списка или набора файлов с оглавлением).

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 Skype, ICQ, и других IM-клиентов), а также информацию по связям текущего пользователя за указанный период времени.

Подсистема должна предоставлять возможность просмотра информации по активности сотрудников в режиме реального времени с возможностью фильтрации по категориям активности пользователя.

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.

Подсистема должна предоставлять возможность генерации отчетов по имеющимся базовым шаблонам (не менее 30 штук), а также предусматривать возможность добавления пользовательских шаблонов.

Подсистема должна поддерживать предоставление отчетов в табличном, диаграммном, в виде временного графика, а также в виде графа связей.

Подсистема должна производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности.

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.

Подсистема должна генерировать краткие и детальные отчеты по продуктивности работы пользователей за выбранный период времени.

Подсистема должна 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.

Подсистема должна генерировать отчеты по устройствам: перечень установленного оборудования на компьютерах пользователей и отчет по изменениям в устройствах (комплектующих) компьютеров.

Подсистема должна генерировать системные отчеты, отображающие:

- 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.

Подсистема должна предоставлять возможность быстрого перехода к поиску и просмотру найденных документов.

Подсистема должна предоставлять возможность переходов по связанным отчетам.

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.

Подсистема должна обеспечивать получение наглядного представления об адресах, с которых выбранный пользователь отправлял либо на которые получал сообщения.

Подсистема должна предусматривать возможность конвертации сгенерированных отчетов в PDF-файл, равно как и вывод их на печать.

Подсистема должна предоставлять функциональную возможность для расследования аудиторами инцидентов безопасности, позволяющую создавать задачи с прикрепленными к ним результатами поиска и файлами, назначать аудитора, ответственного за их решение, а также устанавливать приоритет и срок выполнения задач.

5.2. Требования к подсистеме принятия решений

Подсистема должна использовать клиентскую консоль для управления политиками безопасности и инцидентами. Для консоли должно работать изолированное разграничение прав доступа.

Подсистема должна выносить единый вердикт (инцидент / не инцидент) для каждого перехваченного объекта.

Подсистема должна предоставлять возможности для ведения журнала инцидентов с возможностью рубрикации по каналам передачи данных, протоколам, пользователям, правилам проверки.

Подсистема должна предоставлять возможность уведомления ответственных лиц об инцидентах по электронной почте.

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).

Подсистема должна предоставлять возможности для изменения существующих и применения новых правил автоматического вынесения вердикта (правил проверки).

Подсистема должна предусматривать возможность применения пользовательских шаблонов политик безопасности (правил проверки).

Подсистема должна предоставлять возможность выполнения ретроспективного контроля перехваченных документов с учетом обновленных правил проверки.

Подсистема должна предусматривать возможность объединения политик безопасности (правил проверки) в группы.

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.

Подсистема должна предоставлять возможности для использования «белых» списков исключений (списки пользователей, документы которых исключены из проверок) и «черных» списков исключений (списки пользователей, только по документам, которых будет проводиться проверка).

Подсистема должна предоставлять возможность экспорта/импорта структуры настроек (политик безопасности, критериев поиска, списков исключений и др.).

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.

Подсистема должна предоставлять возможности протоколирования выявленных инцидентов.

Подсистема должна поддерживать возможность категоризации инцидентов с помощью цветовых меток.

Подсистема должна поддержать возможность экспорта данных об инцидентах и событиях посредством syslog.

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.

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.

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);
- по количественным показателям статистических запросов (числу отправленных писем/распечатанных страниц/сообщений в Skype, Lync, Viber, IM и пр.);
- возможность сузить результаты поиска путем дополнительного поискового запроса (фильтры по найденному).

Подсистема должна предусматривать наличие в дистрибутиве нескольких словарей.

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.

Подсистема должна предоставлять возможности для просмотра детальной информации по каждому инциденту.

5.3. Требования к подсистеме контроля

5.3.1. Общие требования к функциям Агента для ОС Windows

5.3.1.1. Требования к модулю контроля электронной почты

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.

Модуль должен предоставлять возможность блокировки исходящей почты по контентным и/или контекстным критериям на почтовом сервере без необходимости установки модуля контроля (работа в разрыв).

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.

5.3.1.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

Модуль должен обеспечивать контроль:

- входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), XMPP (Jabber), MMP (Агент Mail.ru), и др, на усмотрение Разработчика Системы;
- входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и прочее на усмотрение Разработчика Системы);
- чатов, файлов, переданных при помощи desktop-версий мессенджеров: Skype, Lync, Viber, Telegram, WhatsApp, Rocket.chat, Mattermost;
- чатов, файлов веб-версий мессенджеров: Skype (web.skype.com), Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost, Teams, Bitrix24;
- чатов, звонков и файлов, переданных при помощи Zoom Chat, TrueConf Client, а также конференций Zoom;
- истории передачи файлов и чатов Instagram, LINE, Output Messenger;
- сообщений и файлов ресурса slack.com.

Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту, передаваемых по протоколу HTTP в социальных сетях, посредством Slack, Zoom Chat, Telegram, а также возможность блокировки

файлов, передаваемых посредством WhatsApp Desktop, WhatsApp Web и полной блокировки доступа к Telegram Web.

Модуль должен осуществлять контроль сеансов текстовой и голосовой связи (в том числе, звонки на телефонные номера и звуковые дорожки сеансов видеосвязи), файлов и SMS-сообщений, переданных при помощи Skype.

Модуль должен обеспечивать контроль входящих/исходящих сообщений, звонков и файлов коммуникационных программ-клиентов Microsoft Lync, Viber и Telegram.

Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN'ов отправителя и получателей, количества сообщений и др.

5.3.1.3. Требования к модулю контроля FTP-соединений

Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединения, в том числе с применением SSL-шифрования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.

Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище.

5.3.1.4. Требования к модулю контроля HTTP-трафика

Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).

Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome.

Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.

Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).

Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.

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.

Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков исключений, 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.

Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

5.3.1.5. Требования к модулю контроля печати

Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров.

Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др.

Модуль должен поддерживать возможность исключения из контроля отдельных принтеров (в том числе по их описанию и месту расположения), пользователей, документов (по именам) и процессов.

Модуль должен обеспечивать возможность блокировки печати файлов, соответствующих определенному контенту и/или контексту.

Модуль должен позволять блокировку Escape-функций для PostScript/PCL принтеров, при активации которых контроль распечатанных документов невозможен.

5.3.1.6. Требования к модулю контроля съёмных устройств

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, SCSI и прочее на усмотрение Разработчика Системы).

Модуль должен поддерживать работу в терминальной сессии.

Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.

Модуль должен предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство.

Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве.

Модуль должен предоставлять возможность теневого копирования данных, передаваемых через буфер обмена, в том числе буфер обмена RDP-сессии.

Модуль должен предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе.

Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».

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.

Модуль должен предоставлять возможность запрета копирования данных, передаваемых через RDP-сессию.

Модуль должен позволять ограничение установки RDP-подключения как на удаленные рабочие станции или серверы, так и на рабочую станцию или сервер с работающим модулем.

Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя.

Модуль должен предоставлять возможность блокировки Bluetooth-устройств и сервисов.

Модуль должен предоставлять возможность контроля буфера обмена на компьютере пользователя, а также блокировку передачи данных через буфер обмена по содержимому копируемых данных.

Модуль должен предоставлять возможность блокировки доступа пользователей к определенным локальным папкам и/или логическим дискам (за исключением системных).

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.

Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.

5.3.1.7. Требования к модулю контроля событий на мониторах и действий сотрудников

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.

Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, звонке или активации видеоконференции Skype, отсутствии активности от клавиатуры и мыши, нажатии клавиши «PrintScreen» или сочетания клавиш Win+Shift+S.

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.

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.

Модуль должен позволять скорректировать расписание создания снимков при посещении определенных (настроенных заранее) интернет-узлов, авторизации в операционной системе, отсутствии пользовательских сессий.

Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи.

Модуль должен обеспечивать одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени.

Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры в режиме реального времени.

Модуль должен предоставлять возможность экспорта перехваченных снимков экрана и видеозаписей в отдельную папку.

Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.

Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.

Модуль должен обеспечивать возможность блокировки нажатий клавиши «PrintScreen».

Модуль должен выделять и позволять исключать из аудита набранные символы, если они являются вводом пароля для всех случаев, когда это технически возможно. Техническая возможность определяется Разработчиком Системы.

Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

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.

Модуль должен предоставлять возможность экспорта перехваченных нажатий клавиш в отдельную папку.

Модуль должен предоставлять возможность добавления перманентных водяных знаков на изображения экранов мониторов пользователей с возможностью изменения прозрачности водяных знаков и их отображения на создаваемых снимках и видеозаписях.

5.3.1.8. Требования к модулю контроля разговоров сотрудников

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.

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.

Модуль должен обеспечивать возможность прослушивания подключенного к рабочей станции микрофона в режиме реального времени.

Модуль должен обеспечивать помещение записанных звуковых файлов в базу данных либо использовать для хранения бинарных данных файловое хранилище.

Модуль должен предоставлять возможность экспорта перехваченных разговоров в отдельную папку.

5.3.1.9. Требования к модулю контроля активности пользователей и приложений

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

Модуль должен иметь подключаемую возможность автоматической категоризации любых посещенных сайтов на тематические группы, используя заранее загруженную и регулярно пополняемую базу классификации сайтов.

5.3.1.10. Требования к модулю контроля облачных хранилищ данных

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, Диск-О и другие на усмотрение Разработчика Системы.

Модуль должен обеспечивать контроль файлов, передаваемых в программах удаленного доступа TeamViewer, RealVNC, Radmin, LiteManager и другие на усмотрение Разработчика Системы.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др.

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.

5.3.1.11. Требования к модулю аудита файлов

Модуль должен предоставлять возможности:

- локального сканирования файлов посредством Агента Системы, установленного на рабочую станцию с клиентской либо серверной операционной системой семейства Windows;
- сетевого сканирования без установки Агента Системы путем подключения источников по протоколам:
  - SMB;
  - FTP и FTPs;
  - SSH (SFTP);
  - WebDAV.
- сканирования содержимого электронных писем на серверах Microsoft Exchange;
- аудита операций с файлами с использованием функций Агента, а также с использованием функции чтения журналов событий Windows и/или NetApp;
- получение информации об изменениях на контроллере домена через журнал безопасности Active Directory.

Модуль должен иметь возможность использования технологии OCR как на Агенте, так и на сервере с возможностью использования отдельного сервера OCR при сетевом сканировании.

Модуль должен протоколировать файлы, статически хранящиеся, создаваемые, изменяемые на рабочих станциях пользователей.

Модуль должен обеспечивать возможность выборки протоколируемых ресурсов (рабочие станции, файл-серверы, FTP-серверы, почтовые серверы, отдельные жесткие диски и папки).

Модуль должен обеспечивать регистрацию следующих событий с файлами: создание, чтение, запись, удаление, переименование, выполнение, изменение расширения, перемещение, копирование, запрет доступа, изменение прав доступа.

Модуль должен обеспечивать сканирование содержимого файлов на локальных и сетевых файловых системах, FTP-серверах, почтовых серверах в соответствии с настроенными правилами сканирования.

Модуль должен предоставлять возможность применения предустановленных шаблонов правил сканирования с возможностью их редактирования.

Модуль должен обеспечивать присваивание зафиксированным операциям с файлами следующих атрибутов: доменных учетных записей, вид произведенной над файлом операции, имя и тип файла, путь к файлу и др.

Модуль должен предоставлять возможность исключения из аудита системных пользователей.

Модуль должен предоставлять возможность указания перечня процессов и файлов (в том числе системных и временных), которые будут исключены из аудита или наоборот – включены в него.

Модуль должен предоставлять возможность передачи запротоколированной информации подсистеме контентного анализа.

Модуль должен обеспечивать присваивание меток файлам, которые соответствуют настроенным правилам сканирования, а также позволять устанавливать метки ручной классификации (метки конфиденциальности документа).

Модуль должен позволять управлять правами пользователей по изменению/назначению/удалению меток конфиденциальности.

Модуль должен иметь возможность оповещать пользователя о необходимости установки метки конфиденциальности на создаваемый файл офисного пакета Microsoft Office и/или AutoCAD.

Модуль должен автоматически присваивать метку конфиденциальности файлу офисного пакета Microsoft Office и/или AutoCAD в соответствии с заданными администратором правилами.

Модуль должен предоставлять возможность блокировки доступа указанных процессов/пользователей/компьютеров к файлам, имеющим соответствующую метку.

Модуль должен предоставлять возможность отображать в интерфейсе пользователя на рабочей станции с агентом сообщение о блокировке файла с меткой, который пытается открыть пользователь.

Модуль должен обеспечивать возможность создания указанного количества архивных копий файла, содержимое которого удовлетворяет настроенным правилам сканирования, с целью отслеживания истории изменений файла.

Модуль также должен обеспечивать возможность восстановления архивных копий файлов из архива системы.

Модуль должен поддерживать регистрацию прав доступа к файлам и папкам сетевых и локальных файловых систем (за исключением мандатных схем разграничения прав).

Модуль должен обеспечивать отображение структуры файловой системы в виде дерева файлов и папок, аналогичное дереву на сканируемой рабочей станции или сервере.

Модуль должен предоставлять возможность минимизировать нагрузку на конечную рабочую станцию посредством гибкой настройки параметров:

- Скорость/приоритет сканирования;
- Расписание сканирования;
- Приоритет сканирования при простое системы;
- Ограничение вычислительной нагрузки.

Модуль должен предоставлять возможность создания правил сканирования с использованием поисковых технологий:

- Атрибутивных (поиск файлов по значениям атрибутов: размер, дата создания, директория, расширение и др.);
- Текстовых (поиск документов, содержащих определенные слова, фразы) с учетом морфологии и транслитерации;
- По словарю (поиск документов, содержащих определенное количество либо процент слов из словаря);
- Поиск похожих (поиск документов по образцу текста, схожему по смыслу или содержанию с искомым, с возможностью указания процента релевантности (схожести) документов);
- Регулярных выражений (поиск файлов, содержащих заданные цифробуквенные последовательности, например, номер паспорта, номер кредитной карты и т.д.);
- Меткам ручной классификации (поиск файлов, содержащих установленные метки ручной классификации);
- По меткам других приложений (поиск файлов, содержащих установленные метки Microsoft Information Protection);
- Любых комбинаций вышеперечисленного.

Модуль должен предоставлять возможность выделения файлов, удовлетворяющих правилам сканирования, соответствующими графическими пиктограммами с указанием конкретного правила сканирования. В случае, если файл удовлетворяет нескольким правилам сканирования, модуль должен отображать все критерии.

В модуле должна быть предусмотрена возможность фильтрации (например, отобразить только файлы, удовлетворяющие определенным критериям сканирования; отобразить файлы и папки, доступные определенной группе пользователей и т.д.).

Модуль должен предоставлять возможность дополнять отчеты историей файловых операций.

Модуль должен обеспечивать отслеживание изменений файлов и высокую частоту переиндексации информации (данные операции применяются только к новым файлам и файлам, измененным с момента последней индексации) и обеспечивать возможность сохранения теневой копии данных в случае, если те умышленно удалены пользователем.

Модуль должен предоставлять возможность бесшовной интеграции с другими модулями подсистемы контроля, что позволит строить контентные маршруты и переходить к оригинальным сообщениям, если файл был отправлен или получен посредством контролируемых каналов коммуникации.

Модуль должен иметь возможность интеграции с сервисом EveryTag, обеспечивающим внедрение информации в файлы формата PDF в соответствии с политиками, заданными в EveryTag.

5.3.2. Общие требования к функциям Агента для ОС Linux

Агент для ОС Linux должен осуществлять контроль данных, передаваемых посредством электронной почты, сервисов обмена мгновенными сообщениями, FTP-соединений, протокола HTTP, сервисов облачных хранилищ, контроль и управление доступом к данным на внешних устройствах, контроль печати данных, событий на мониторах и их действий, разговоров сотрудников и их активности в приложениях, а также контроль файлов, статически хранящихся на рабочих станциях сотрудников.

5.3.2.1. Требования к модулю контроля электронной почты

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 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.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.

5.3.2.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

Модуль должен обеспечивать контроль:

- входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), XMPP (Jabber), MMP (Агент Mail.ru), SIP (X-Lite и др.) и др.;
- входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и прочее на усмотрение Разработчика Системы);
- чатов, звонков, исходящих файлов, переданных при помощи desktop-версии Telegram;
- чатов, исходящих файлов веб-версий мессенджеров: Skype (web.skype.com), Bitrix24;
- чатов веб-версий мессенджеров: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com).

Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN'ов отправителя и получателей, количества сообщений и др.

5.3.2.3. Требования к модулю контроля FTP-соединений

Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединение, в том числе с применением SSL-шифрования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.

5.3.2.4. Требования к модулю контроля HTTP-трафика

Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).

Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Mozilla Firefox; Opera; Google Chrome.

Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.

Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).

Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

5.3.2.5. Требования к модулю контроля печати

Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров.

Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др.

Модуль должен поддерживать возможность исключения из контроля отдельных принтеров (в том числе по их описанию и месту расположения), пользователей.

5.3.2.6. Требования к модулю контроля и управления доступом съёмных устройств

Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (съемные накопители USB, Wi-Fi и сетевым папкам, модемам и сетевым адаптерам) и портам (COM, LPT).

Модуль должен поддерживать работу в терминальной сессии.

Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.

Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве или записываемых на внешнее USB-устройство.

Модуль должен предоставлять возможность фиксирования всех событий в журнале аудита: создание, открытие, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе.

Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».

Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.

5.3.2.7. Требования к модулю контроля событий на мониторах и действий сотрудников

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.

Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, запуске определенных (настроенных заранее) процессов, отсутствии активности от клавиатуры и мыши, нажатии клавиши «PrintScreen».

Модуль должен обеспечивать видеозапись происходящего на экранах мониторов. Модуль должен позволять останавливать запись экрана при отсутствии активности от клавиатуры и мыши рабочей станции.

Модуль должен обеспечивать создание снимков посредством подключенной к рабочей станции веб-камеры по заданному расписанию, в том числе при входе пользователя в операционную систему, с возможностью использования нескольких веб-камер.

Модуль должен обеспечивать просмотр активности экрана пользователя в режиме реального времени.

Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры в режиме реального времени.

Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент создания снимка экрана.

Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.

Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.

Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

5.3.2.8. Требования к модулю контроля разговоров сотрудников

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.).

Модуль должен обеспечивать возможность прослушивания подключенного к рабочей станции микрофона в режиме реального времени.

Модуль должен предусматривать возможность активации записи голосов по расписанию, внутри офиса/за его пределами (в командировке), а также возможность настройки качества записываемого звукового файла.

5.3.2.9. Требования к модулю контроля активности пользователей и приложений

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

5.3.2.10. Требования к модулю контроля облачных хранилищ данных

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.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др.

5.3.2.11. Требования к модулю аудита файлов

Модуль должен предоставлять возможности:

- локального сканирования файлов посредством Агента Системы, установленного на рабочую станцию с операционной системой семейства Linux;
- аудита операций с файлами с использованием функций Агента.

Модуль должен обеспечивать регистрацию следующих событий с файлами: создание, чтение, запись, удаление, переименование.

Модуль должен обеспечивать присваивание зафиксированным операциям с файлами следующих атрибутов: учетных записей, вид произведенной над файлом операции, имя и тип файла, путь к файлу и др.

Модуль должен предоставлять возможность аудита прав доступа к файлам и папкам файловой системы

Модуль должен предоставлять возможность исключения из аудита операций, производимых от имени системной учетной записи (например, действия антивирусов, систем резервного копирования и т.д.).

Модуль должен предоставлять возможность указания перечня процессов и файлов (в том числе системных и временных), которые будут исключены из аудита или наоборот – включены в него.

Модуль должен обеспечивать присваивание меток файлам, которые соответствуют настроенным правилам сканирования.

Модуль должен протоколировать файлы, статически хранящиеся, создаваемые, изменяемые на рабочих станциях пользователей.

Модуль должен обеспечивать возможность создания указанного количества архивных копий файла, содержимое которого удовлетворяет настроенным правилам сканирования, с целью отслеживания истории изменений файла.

5.3.3. Общие требования к функциям Агента для ОС MacOS

Агент для ОС MacOS должен осуществлять контроль событий на мониторах и действий сотрудников, их активности в приложениях, а также контроль файлов, статически хранящихся на рабочих станциях сотрудников.

5.3.3.1. Требования к модулю контроля событий на мониторах и действий сотрудников

Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции.

Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент создания снимка экрана.

Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.

Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.

Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

5.3.3.2. Требования к модулю контроля активности пользователей и приложений

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

5.3.3.3. Требования к модулю индексации файлов рабочих станций

Модуль должен обеспечивать отслеживание изменений файлов и высокую частоту переиндексации информации. Данные операции применяются только к новым файлам и файлам, измененным с момента последней индексации.

Модуль должен обеспечивать возможность сохранения теневой копии данных в случае, если те умышленно удалены пользователем.

5.3.4. Требования к функциям контроля данных на уровне сетевого перехвата (при интеграции с прокси-сервером (по протоколу ICAP) либо сетевым оборудованием через зеркалирование трафика (SPAN))

5.3.4.1. Требования к модулю контроля электронной почты

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.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.

5.3.4.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

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, Мой Мир@Mail.ru, Одноклассники.ru, 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.

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.

Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN'ов отправителя и получателей, количества сообщений и др.

5.3.4.3. Требования к модулю контроля FTP-соединений

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

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.

Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище.

5.3.4.4. Требования к модулю контроля HTTP-трафика

Контроль защищенного HTTPS трафика может быть доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата.

Контроль незащищенного HTTP трафика может быть доступен как режиме интеграции с прокси-сервером, так и в режиме зеркалирования трафика.

Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).

Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome.

Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.

Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).

Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.

Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков исключений, 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.

Модуль должен обеспечивать возможность блокировки передачи запросов, соответствующих определенному контексту.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

5.4. Требования к системе мониторинга

В системе мониторинга должна быть возможность собирать информацию об уязвимостях, мониторить метрики систем и сервисов на серверах, а также контролировать доступность служб с использованием специализированных агентов:

- Система должна уметь собирать данные, связанные с безопасностью, с конечных устройств, включая журналы событий безопасности, журналы приложений и другие.
- Система должна мониторить поведение и активность на конечных устройствах для выявления подозрительных действий.
- Система собранные данные должна отправлять на сервер для анализа и выявления потенциальных угроз безопасности.

- Система должна иметь механизмы для сообщения о выявленных событиях безопасности на сервере для принятия мер по реагированию.
- В системе должна быть возможность анализа сетевого трафика в реальном времени и записи транзакций и коммуникации между устройствами.
- Система должна предоставлять информацию о соблюдении стандартов и нормативов, таких как PCI DSS, GDPR и HIPAA.
- Система должна поддерживать множества операционных систем: Агент должен быть способен работать на различных операционных системах, включая Linux, Windows, macOS и другие.

В системе должно быть реализована защита данных путем шифрования связи с сервером.

Система мониторинга должна уметь проводить «парсинг» приходящие к ней события. Под «парсингом» событий понимается процесс анализа событий и распределения на отдельные компоненты в отдельных полях в соответствии с исходными данными, например: исходный IP-адрес, конечный IP-адрес, дата, время, исходный пользователь, целевой пользователь, содержимое события и т. д. Этот процесс должен выполняться с использованием правил синтаксического анализа.

Система мониторинга должна обеспечивать возможность быстрого добавления поддержки новых источников данных на случай, если возникнет необходимость добавить источник, который до сих пор не поддерживался. В системе должна быть предусмотрена возможность создания собственных правил парсинга для анализа поступающей в систему информации на основе регулярных выражений.

В системе должен быть предусмотрен сбор логов из любой таблицы в базах данных (обязательно Microsoft SQL и Oracle) и их дальнейшая обработка.

Предлагаемое решение должно обеспечивать сбор событий с серверов с операционными системами Microsoft Windows и Unix/Linux, без необходимости дополнительных расходов или содержать соответствующий лицензионный пакет, гарантирующий возможность сбора из потенциальных источников, которые захочет Заказчик и возможность подключения этих источников к системе.

Система мониторинга должна иметь возможность создавать свои собственные правила корреляции. Создание корреляционной логики должно быть основано на графическом интерфейсе (построение логики на основе логических блоков, блоков ветвления и условий, а также блоков, представляющих данные).

Решение должно обеспечивать возможность объединения сетевых событий и потоков. Агрегация должна объединять похожие события в одно коллективное событие.

Система мониторинга должна собирать сетевые потоки (Netflow) и журналы, анализировать и суммировать их в согласованном формате и разделять (нормализовать) их на категории, по крайней мере, такие как ведение журнала, выход из системы, вредоносное ПО, эксплойт, разведка, сканирование портов и т.д.

Должна быть возможность назначать уведомления конкретному пользователю или группе пользователей. Также должен быть предусмотрен механизм эскалации адресата уведомления по истечении определенного периода времени.

Архитектура предлагаемого решения должна позволять реализацию в распределенной среде.

Архитектура предлагаемого решения должна позволять реализацию в распределенной среде.

Система должна иметь возможность определять специальные списки объектов, которые могут содержать как минимум следующие объекты: IP-адреса, пользователей, домены, MAC-адреса, географические местоположения и любые строки символов.

В системе должен быть API, позволяющий обновлять список объектов актуальной информацией. Например, сценарий, создающий список IP-адресов, которые необходимо учитывать для корреляции, должен иметь возможность внедрить этот список непосредственно в решение.

Если доступ к API является дополнительным платным элементом, он должен быть включен в предлагаемую систему.

Обновление ПО системы должно производиться без физического доступа к устройствам.

Веб-интерфейс должен поддерживать мульти-языковую локализацию (английский и другие языки по требованию Заказчика).

Модуль анализа поведения пользователей (UEBA) должен обеспечивать динамическую оценку рисков для каждого пользователя на основе их активности. Система должна автоматически категоризировать пользователей по уровням риска (например, низкий, средний, высокий) с визуализацией этих данных.

AI-модели должны поддерживать обучение на основе исторических данных системы, обеспечивая прогнозирование событий, таких как возможные сбои в инфраструктуре или потенциальные инциденты безопасности.

Модуль Network Probe должен иметь возможность взаимодействовать с репутационными базами данных, выявляя подозрительные IP-адреса и вредоносные сетевые активности.

6. Прочие требования ко всему программному обеспечению

6.1. Требования к услугам по установке и настройке

Поставщик должен выполнить установку каждой составной части приобретенного решения в течение до тридцати (30) дней после поставки. Услуги выполняются на условиях «под ключ».

6.2. Требования к лицензированию программного обеспечения

Все лицензии должны быть выданы на бессрочное использование, то есть по истечении 36 (тридцати шести) месяцев обновления и гарантии продукты будут продолжать использоваться контрагентом, независимо от того, приобретаются ли пакеты обновлений и техническая поддержка для последующего использования.

Участник конкурса должен представить доказательство, выданное производителем каждого предлагаемого компонента программного обеспечения, информирующее о том, что поставщик может и уполномочен продавать продукты и услуги на территории Республики Узбекистан.

Участник конкурса должен представить сертификат выданный программному обеспечению, выполняющему функции DLP и файлового аудита, со стороны организации «Центр Кибербезопасности» Узбекистана, согласно требованиям нормативной документации O'z DSt 2816:2014 п. 5.3 (3 уровень отсутствия НВД) и O'z DSt 2814:2014 п.9.1, п.9.2, п.9.4.

Участник конкурса должен предоставить подтверждение об освобождении от налога на доходы нерезидента в соответствии с законодательством Республики Узбекистан:

- Участник должен подтвердить, что является резидентом *указать страну резидентства*, как компания, зарегистрированная в *указать страну резидентства*, и юридическим лицом *указать страну резидентства*, имеющим право на льготы по Соглашению между *указать страну резидентства* и Правительством Республики Узбекистан об избежание двойного налогообложения в отношении налогов на доходы, ратифицированному *указать дату и номер межправительственного соглашения*.
- Участник конкурса в составе пакета квалификационных документов должен предоставить сертификаты, оформленные должным образом, подтверждающие, что он является налоговым резидентом *указать страну резидентства*.
- Участник конкурса в составе пакета квалификационных документов должен предоставить сертификаты, оформленные должным образом, подтверждающие, что правообладатель предлагаемых программных продуктов является налоговым резидентом *указать страну резидентства*.
- Освобождение от уплаты налога на доходы (прибыль) нерезидента в применимых в соответствии с законодательством РУз производится на основании следующих документов:

- справка (сертификат) о резидентстве участника конкурса в одном экземпляре;
- справка (сертификат) о резидентстве правообладателя предлагаемых программных продуктов в одном экземпляре.

- В случае непредоставления Исполнителем вышеуказанных Справок о резидентстве, Заказчик производит оплату по настоящему договору с удержанием налога на доходы нерезидентов в размере 20% по тому программному продукту, на который не был предоставлен соответствующий Сертификат резидентства правообладателя и Сертификат резидентства участника конкурса.

6.3. Дополнительные требования

В состав предложения участника конкурса должно быть включено авторизованное обучение по всем программным продуктам– 2 сотрудника.

Внедрение всех систем на условиях «под ключ» и поддержка в течение срока действия гарантии.

Техническая поддержка правообладателя/производителя на все программное обеспечение, предлагаемое в рамках текущего конкурса – 3 года.

Внесено:

Заместитель директора департамента безопасности и защиты информации **Б.Б.Шамсиев**