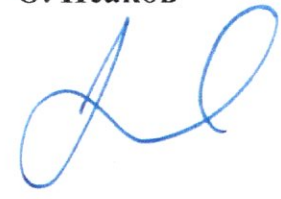
УТВЕРЖДАЮ

Заместитель министра финансов

Республики Узбекистан

О. Исаков



Техническое задание

На модернизацию автоматизированной системы защиты конфиденциальной информации, включая поставку лицензий

1 Перечень сокращений

CD	Compact Disc. Оптический носитель информации в виде пластикового диска с отверстием в центре, процесс записи и считывания информации с которого осуществляется при помощи лазера. Может содержать до 702 МБ данных.
DVD	Digital Versatile Disc. Оптический носитель информации, выполненный в форме диска, для хранения различной информации в цифровом виде. От CD отличается возможностью хранить до 4,7 ГБ данных.
HTTP	HyperText Transfer Protocol. Протокол прикладного уровня передачи произвольных данных.
ICAP	Internet Content Adaptation Protocol. Легкий HTTP-подобный протокол, который используется для расширения функционала прокси-серверов.
IMAP4(S)	Internet Message Access Protocol. Протокол прикладного уровня для доступа к электронной почте.
IP	Internet Protocol. Маршрутизируемый протокол сетевого уровня.
LDAP	Lightweight Directory Access Protocol. протокол прикладного уровня для доступа к службе каталогов.
MAPI	Messaging Application Programming Interface. Программный интерфейс обработки сообщений от компании Microsoft, позволяющий приложениям работать с различными системами передачи электронных сообщений.
MTP	Media Transfer Protocol. Аппаратно-независимый протокол, разработанный компанией Microsoft для подключения цифровых плееров к компьютеру.
NRPC	Notes Remote Procedure Call. Протокол взаимодействия клиента Lotus Notes и сервера Lotus Domino.
OCR	Optical Character Recognition. Оптическое распознавание символов.
POP3(S)	Post Office Protocol Version. Стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению.
PTP	Picture Transfer Protocol. Протокол передачи изображений, создан для того, чтобы выполнять передачу изображений с камеры или телефона Android на компьютер, либо принтер для печати.

SIEM	Security Information and Event Management. Объединение двух терминов, обозначающих область применения ПО: SIM – управление информацией о безопасности, и SEM – управление событиями безопасности.
SMTP(S)	Simple Mail Transfer Protocol. Широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.
TCP	Transmission Control Protocol. Один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных.
TLS	Transport Layer Security. Криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет.
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
КИ	Конфиденциальная информация
ПО	Программное обеспечение

2 Общие требования

2.1 Назначение Системы защиты КИ

Система защиты КИ предназначена для автоматизации деятельности персонала Заказчика, направленной на обеспечение информационной безопасности (далее ИБ), в части обнаружения и реагирования на события ИБ, возникающие в процессе обработки, хранения и перемещения конфиденциальной информации для предупреждения утечки КИ.

2.2 Поставка лицензий

Поставка лицензий на Автоматизированную систему защиты конфиденциальной информации (далее Система защиты КИ) в Министерство Финансов (далее Заказчик). Необходимое количество 400 лицензий.

2.3 Сроки поставки лицензий

Сроки поставки лицензий и выполнения работ по Системе защиты КИ должен составлять не более 90 рабочих дней.

2.4 Требования к поставке лицензий на Систему защиты КИ

В рамках поставки лицензий Заказчику должно предоставляться право на использование Системы защиты КИ, на получение доступа к ресурсу «База знаний» содержащего в себе упорядоченный набор технической, эксплуатационной и другой информационной документации о продуктах , на получение уведомления о выходе новых версий ПО и их особенностях, на право использования всех предоставленных ему новых версий, на получение всех необходимых действий по исполнению процедур коррекции ошибок и/или восстановления работоспособности Системы защиты КИ и на получение обновлений для Системы защиты КИ.

Срок подписки на обновления Системы защиты КИ, в рамках данного проекта, должен составлять не менее 1 года, с момента окончания реализации проекта.

2.5 Требования к гарантийным обязательствам

Исполнитель гарантирует наступление даты окончания поддержки поставляемого решения не ранее чем через 5 лет с момента заключения договора поставки решения.

В рамках выделенного бюджета Исполнитель должен предоставить полностью укомплектованное и работоспособное решение, при необходимости предложить дополнительные модули, продукты и услуги по каким-либо причинам неучтенные Заказчиком, но обязательные для обеспечения полноты использования запрашиваемой конфигурации.

3 Требования к Исполнителю (подрядчику)

Исполнитель должен иметь партнерский статус с производителями программного обеспечения, которое будет использоваться для построения Системы (для подтверждения соответствия данному требованию Исполнитель должен предоставить копии соответствующих сертификатов и писем).

Исполнитель должен обеспечить для реализации проекта проектную команду, состоящую из специалистов с подтверждением их квалификация.

Исполнитель (участник):

- предоставляет информации по:
  - персональному составу проектной команды (подтверждение наличия в штате исполнителя специалистов (инженеров), квалификация которых подтверждена соответствующими сертификатами);
  - методам достижения минимального уровня TCO (Total Cost of Ownership) сроком на не менее 5 лет;
  - сервисам и подпискам;
  - условиям лицензирования при наличии (объем предоставления, порядок взимания платы, срок действия лицензий и др.);
  - перечню осуществляемых работ (услуг) с конкретизацией объема и привлекаемых специалистов (обоснование формирования стоимости оказываемых услуг);

Исполнитель должен предпринять все необходимые меры по обеспечению информационной безопасности и сохранности конфиденциальной информации, а также, предотвращению утечки информации.

4 Требования к Системе защиты КИ

4.1 *Требования к Системе защиты КИ в целом*

Установка Системы защиты КИ в существующую вычислительную сеть Заказчика не должна накладывать ограничений на нормальное функционирование серверов и рабочих станций Заказчика.

Система защиты КИ должна обеспечивать возможность контроля не менее 400 учётных записей пользователей:

Система защиты КИ должна иметь консоль проведения расследований и предоставления отчётности на русском языке через web-интерфейс.

Исполнитель в рамках выделенного бюджета, может предложить аналогичное/альтернативное либо с превосходящими характеристиками решение, которое будет выполнять все поставленные цели и задачи, указанные в настоящем техническом задании (с учетом целевого назначения и показателей). Для соответствия техническому заданию допускается установка опциональных модулей (в том числе взаимоинтегрированные), имеющихся в линейке разработчиков решения.

4.1.1 Требования к способам и средствам связи для информационного обмена

Система защиты КИ должна функционировать в составе информационно-вычислительной сети Заказчика.

Система должна корректно работать в распределенных сетях.

Для информационного обмена между компонентами Системы защиты КИ должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet).

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

Должна быть возможность использовать Систему защиты КИ в структуре филиалов, в т.ч. при низкой пропускной способности каналов связи между филиалами, выделении канала связи для передачи данных между компонентами системы по расписанию (например, только ночью) и возможными обрывами соединения.

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

4.1.2 Требования к характеристикам взаимосвязей

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

Система защиты КИ должна обеспечивать возможность интеграции со следующими proxy-серверами: Aladdin eSafe, Bluecoat ProxySG, Check Point, Cisco IronPort, FortiGate, Squid, SurfSecure, Vaultize, UserGate UTM и другими proxy-серверами с поддержкой ICAP.

Система защиты КИ должна обеспечивать возможность контроля загрузки и создания документов в облачном сервисе (системе/приложении/хранилище) Microsoft Office (OneDrive/SharePoint) при интеграции с Microsoft Cloud App Security по протоколу ICAP.

Система защиты КИ должна обеспечивать возможность получения копии писем, отправленных в облачном сервисе Microsoft Exchange Online.

Система защиты КИ должна обеспечивать возможность хранения всех данных в исходном виде в течение (срок) 1 год

4.1.3 Требования к режимам функционирования Системы защиты КИ

Система защиты КИ должна функционировать в автоматизированном режиме под управлением администратора.

Система защиты КИ 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 защиты КИ или с внешними сетями, для доступа к конфигурационной и архивной информации.

4.1.4 Требования по диагностированию Системы защиты КИ

Система защиты КИ должна обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности.

Система защиты КИ должна обеспечивать возможность контроля целостности системных файлов, как в автоматическом, так и в ручном режиме.

4.1.5 Требования к численности и квалификации персонала

Исполнитель должен обеспечить необходимым объемом специалистов для реализации проекта. Персонал Исполнителя должен обладать опытом эксплуатации операционных систем АРМ и серверов, сетевых протоколов, централизованных систем идентификации и аутентификации, систем электронной почты и т.п.

4.1.6 Требования к производительности и надежности

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

Система защиты КИ должна обеспечивать возможность масштабирования и отказоустойчивости, в том числе поддерживать кластерные технологии.

Должно осуществляться резервное копирование и хранение резервных копий данных, с возможностью их восстановления.

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

4.2 Требования к функциональным возможностям Системы защиты КИ

4.2.1 Требования к перехвату трафика

Подсистема перехвата трафика должна обеспечивать контроль действий по отправке информации в ситуации, когда клиент находится вне локальной сети организации. Подсистема перехвата трафика должна извлекать из перехваченных объектов текстовую информацию и вложения, выполнять определение форматов вложений и передачу извлеченных данных в подсистему анализа.

4.2.1.1 Требования к контролю корпоративной почты

Модуль должен осуществлять перехват входящих или исходящих почтовых сообщений, передаваемых по протоколам MAPI, POP3(S), IMAP4(S), SMTP(S) и подготовку этих данных к дальнейшему анализу.

Перехват данных, передаваемых из корпоративной сети по протоколам POP3(S), IMAP4(S), SMTP(S) должен быть возможен без установки клиентского программного обеспечения.

Модуль должен обеспечивать возможность блокировки отправки почтовых сообщений по протоколам MAPI, SMTP(S), HTTP(S) (веб-почта) по результатам анализа содержимого.

Модуль должен предоставлять возможность блокировки отправки почтовых сообщений по результатам анализа содержимого, передаваемых по протоколу SMTP(S), без необходимости установки клиентского программного обеспечения.

Модуль должен предоставлять возможность помещения почтовых сообщений на карантин по результатам анализа содержимого, передаваемых по протоколу SMTP(S), без необходимости установки клиентского программного обеспечения. В случае подтверждения нарушения офицером безопасности сообщения должны блокироваться, в противном случае отправляться адресату.

Модуль должен расшифровывать сообщения, сформированные по стандарту S/MIME, если для передачи используется протокол MAPI и криптографический провайдер Microsoft.

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

4.2.1.2 Требования к контролю web-трафика

Модуль должен обеспечивать перехват загружаемых данных по протоколам HTTP(S) (web-почта, форумы, блоги, чаты и т.д.).

Модуль должен обеспечивать возможность блокировки передачи данных по протоколам HTTP(S) по результатам анализа содержимого.

Модуль должен осуществлять фильтрацию «мусорного трафика» (бесполезных служебных HTTP-запросов) на основании передаваемых данных, их размера и IP-адреса или домена, к которому отправляются эти запросы.

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

4.2.1.3 Требования к контролю мессенджеров

Модуль должен обеспечивать перехват сообщений чатов, файлов, отправленных при помощи сервиса обмена мгновенными сообщениями Telegram и обеспечивать возможность осуществлять разрешение или запрет для пользователей использования сервиса обмена мгновенными сообщениями Telegram.

Модуль должен обеспечивать перехват и обработку сообщений чатов и файлов, отправленных при помощи desktop-приложения и web-версии Skype.

Модуль должен обеспечивать возможность интеграции с сервисом обмена мгновенными сообщениями Microsoft Teams или др., для перехвата сообщений чатов, протоколирования передачи файлов, совершённых при помощи этого сервиса.

Модуль должен обеспечивать возможность перехвата файлов, который пользователь получает или отправляет другим адресатам при использовании desktop приложения сервиса Viber. Модуль должен выполнять выделение транспортных атрибутов (отправитель, получатель) из перехваченных данных.

4.2.1.4 Требования к контролю подключаемых устройств

Модуль должен обеспечивать возможность осуществлять разрешение или запрет для пользователей работы с периферийными устройствами (съёмные носители, принтеры, модемы, различные физические порты и т.д.), в том числе ограничивать доступ только на чтение, предоставлять временный доступ.

Модуль должен обеспечивать возможность создания белых списков устройств, доступ к которым разрешен.

Модуль должен обеспечивать возможность предоставления временного доступа для работы с периферийными устройствами.

Модуль должен обеспечивать возможность запрета создания снимков экрана на рабочей станции пользователя, если снимки создаются стандартными средствами операционной системы.

Модуль должен обеспечивать перехват и обработку данных, передаваемых между съёмным устройством (flash, внешние жёсткие диски, CD/DVD, MTP- и PTP-устройства и т.д.) и защищаемым АРМ, (в т.ч. при редактировании непосредственно на съемных устройствах) с возможностью блокировки передачи данных на съемные USB-устройства хранения по результатам анализа содержимого с помощью лингвистического анализа и детектора текстовых объектов. Модуль должен обеспечивать возможность указания разрешенных имен и идентификаторов съемных устройств, каталогов источника и приёмника копирования для контроля перемещения выбранной категории 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 теневого копирования данных, передаваемых через буфер обмена, в том числе буфер обмена RDP-сессии

Модуль должен обеспечивать возможность блокировки передачи данных через буфер обмена по результатам анализа содержимого с помощью лингвистического анализа и детектора текстовых объектов.

4.2.1.5 Требования к контролю вводимого текста

Модуль должен обеспечивать перехват вводимого с клавиатуры текста, включая текст, копируемый через буфер обмена с возможностью настройки политик перехвата для всех и для настраиваемого списка приложений.

4.2.1.6 Требования к контролю печати документов

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

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

4.2.1.7 Требования к контролю хранения информации

Модуль должен обеспечивать сканирование файлов локальных дисков рабочих станций под управлением Microsoft Windows, сетевых разделяемых ресурсов, файлового хранилища Microsoft SharePoint с использованием следующих параметров: рабочие станции, группы Active Directory, размеры файлов и типы файлов.

Модуль должен обеспечивать сканирование файлов без установки клиентского программного обеспечения.

Модуль должен обеспечивать сканирование файлов следующих облачных хранилищ: Dropbox, OneDrive, Yandex Disk.

4.2.2 Требования к подсистеме анализа

Подсистема анализа должна обеспечивать анализ всех перехваченных данных и их передачу в подсистему применения политик.

Подсистема анализа должна обеспечивать возможность создания комбинированных объектов защиты, описывающих сложные документы с учетом одновременно нескольких технологий анализа, для повышения точности детектирования конфиденциальной информации и уменьшения количества ложных срабатываний.

Подсистема анализа должна предоставлять возможности обработки следующих типов объектов:

1) детектирование по сигнатуре:
   - архивы (7z, exe, xz, lzh, gz, bzip, bz2, tar, arj, rar, zip, zipx, cab, uha, zlib);
   - базы данных (ace, mdb, accdb, dmp);
   - мультимедиа (ape, flac, wma, wmv, asf, mp3, wav, mpg, ogg, avi, m4a, aac, flv, mp4, ai, tif, tiff, wmf, jp2, gif, emf, ppm, wmf, svg, sun, im1, im8, im24, im32, jpeg, jpg, jpe, pbm, png, psd, bmp);
   - исполняемые файлы и библиотеки (rpm, so, exe, dll);
   - другие файлы (xlsb, eml, der, p7s, ink, p7m, otf, torrent, gpg, pgp, gpg, asc, kdb, kdb2, wim);
2) детектирование и извлечение текста:
   - презентации (ppt, pptx, pot, potm, potx, odp);
   - таблицы (xls, xlsx, xlt, xltm, xltx, ods);
   - документы (doc, docx, dot, dotx, docm, odt, pdf, txt, rtf, tsv, csv, stg, json, jsn, chm, pub, vsd, vsdx, html, html, xml, oxps, xps, djv, djvu);
   - почтовые сообщения (tnef, tnf, winmail.dat, msg);
   - другие файлы (odg, mpp, iso, oxps, xps);

Подсистема анализа 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 анализа должна поддерживать следующие кодировки: ISO-8859-1, OEM 866, ISO-8859-5, ISO-8859-15, win-1251, win-1252, koi8-r, utf-8, utf-16.

4.2.2.1 Требования к OCR

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

Модуль должен обеспечивать распознавание текста, содержащегося в изображениях следующих форматов: ai, tif, tiff, pcl, pgm, zjs, wmf, jp2, gif, emf, ppm, wmf, svg, sun, ras, rast, rs, sr, scr, im1, im8, im24, im32, jpeg, jpg, jpe, pbm, png, psd, bmp.

Текст, распознанный модулем OCR, должен анализироваться остальными технологиями анализа.

4.2.2.2 Требования к лингвистическому анализу

Модуль должен выполнять лингвистический анализ с использованием лингвистических алгоритмов:

- 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 мессенджерах и пр.);

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

Модуль должен предоставлять возможность проведения лингвистического анализа для следующих языков: узбекский, русский, английский.

Модуль должен предусматривать возможность настройки индивидуального справочника категорий (классификатора).

4.2.2.3 Требования к модулю детектирования цифровых отпечатков

Для добавляемых пользователем эталонных документов должен формироваться текстовый, бинарный или текстовый и бинарный отпечатки.

Модуль должен поддерживать возможность автоматической синхронизации базы цифровых отпечаток с сетевыми каталогами.

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

4.2.2.4 Требования к модулю детектирования текстовых объектов

Модуль должен выполнять поиск тестовых объектов, соответствующих регулярным выражениям.

Модуль должен содержать предустановленные шаблоны текстовых объектов (ИНН, номер кредитной карты и т.д.). Должны применяться функции верификации текстовых объектов для уменьшения числа ложноположительных срабатываний (например, в номерах банковских карт должны проверяться BIN номер банка и контрольная цифра).

Модуль должен предоставлять возможность добавления текстовых объектов на основе языка регулярных выражений.

4.2.2.5 Требования к модулю детектирования паспортов

Модуль должен позволять отслеживать наличие в поступающих на анализ изображениях главного разворота паспорта гражданина.

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

4.2.2.6 Требования к модулю детектирования печатей

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

Модуль должен предоставлять возможность загрузки эталонных изображений печати для обучения модуля детектирования печатей.

4.2.3 Требования к подсистеме применения политик

Подсистема применения политик должна выполнять вынесение вердикта о факте наличия или отсутствия нарушения перехваченным объектом политики информационной безопасности на основе результатов работы подсистемы анализа. Подсистема должна обеспечивать привязку данных о получателе или отправителе объекта к записям справочника сотрудников и рабочих станций.

Подсистема применения политик должна устанавливать соответствие перехваченных и проанализированных объектов персонам, рабочим станциям и группам, полученным из службы каталогов или созданным пользователем вручную.

Подсистема применения политик должна обеспечивать возможность объединения групп, рабочих станций, web-ресурсов в группы контроля.

Подсистема применения политик должна предоставлять возможности для задания политик безопасности на передачу данных, копирование, хранение данных или использование буфера обмена.

Подсистема применения политик должна предоставлять возможности для автоматического проставления перехваченным объектам дополнительных цветовых меток как на сами политики, так и на документы из консоли управления.

При идентификации перехваченных объектов, прошедших процедуру разбора, должно осуществляться сравнение идентификационной информации, содержащейся в

служебных атрибутах, с идентификационной информацией, полученной из службы каталогов или заданной пользователем Системы защиты КИ.

4.2.3.1 Требования к модулю интеграции со службой каталогов

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

Информационный обмен между Системой защиты КИ и LDAP-каталогом Active Directory должен осуществляться с использованием защищенного протокола LDAPS.

Модуль должен предоставлять возможность настройки периода сканирования измененных элементов. При сканировании измененных элементов в Системе защиты КИ учитываются только изменения, произошедшие с момента последнего сканирования.

Модуль должен предоставлять возможность настройки периода и времени сканирования службы каталогов.

Модуль должен передавать все данные, полученные в результате импорта или синхронизации, в подсистему хранения.

4.2.3.2 Требования к модулю принятия решений

Модуль должен обеспечивать применение политики информационной безопасности путем выполнения для объектов правил, описанных в сценариях их обработки.

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

формальных признаков перехваченного объекта (отправитель, получатель и т.д.), в том числе типа перехваченного объекта (всех типов данных, полученных от подсистемы перехвата трафика);

форматов документов;

Модуль должен обеспечивать возможность информирования администратора безопасности об инцидентах путем отправки письма-уведомления об инциденте на почтовый электронный адрес.

Модуль должен предоставлять возможность определять текст писем-уведомлений офицеру безопасности.

Модуль должен предоставлять возможность определять текст писем-уведомлений для разных политик и вердиктов, примененных к событиям.

Для HTTP(S)-запросов модуль должен определять тип сайта, на который направлен запрос.

Модуль должен предоставлять возможности для передачи объектов в подсистему хранения.

4.2.4 Требования к подсистеме хранения

Подсистема хранения должна обеспечивать хранение всех перехваченных объектов, информации о них, результатов их анализа и применения политик, а также предоставлять возможность для просмотра хранящейся информации посредством запросов из консоли управления.

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

Подсистема хранения должна предоставлять возможность хранения данных на разных физических дисках, например, когда данные за последние 3 месяца хранятся на дисках с более высокой скоростью чтения.

С целью освобождения пространства на жестком диске подсистема хранения должна позволять архивировать сегменты БД хранилища с размещением на других носителях информации, а также обеспечивать возможность их последующего восстановления.

4.2.5 Требования к консолям

Консоль должна предоставлять возможность управления настройками Системы защиты КИ, правами пользователей на работу с функциями Системы защиты КИ, настройки подсистемы анализа, подсистемы применения политик, просмотра информации о перехваченных объектах и выполнения ретроспективного анализа этих объектов.

В консоли должна быть предусмотрена возможность настройки для проведения аудита действий офицера безопасности.

В консоли должен аккумулироваться подробный журнал действий оператора: поисковые запросы, старые и новые значения параметров настроек при их изменении и т.д..

В консоли должна быть предусмотрена возможность по разграничению прав пользователей по работе с функциями Системы защиты КИ на основании ролевой модели.

В консоли должна быть защита от простого создания пароля и перебора пароля.

В консоли должна быть предусмотрена возможность управления доступа к событиям для пользователей Системы защиты КИ.

В консоли должна быть предусмотрена возможность настройки модуля получения детализированных отчетов в интерактивном режиме.

В консоли должна быть предусмотрена возможность отображения детальной карточки события с подсветкой соответствующим цветом обнаруженных в перехваченных данных объектов защиты и терминов.

В консоли должна быть предусмотрена возможность просмотра имеющихся снимков экрана рабочей станции, в том числе связанных с событием из карточки инцидента.

В консоли должна быть предусмотрена возможность проводить полнотекстовый поиск по всем событиям или только по вложениям, с указанием количества получателей, произвольной технологии анализа и канала передачи данных.

В консоли должна быть предусмотрена возможность для подготовки статистических отчетов по перехваченным объектам и их экспорта в следующие форматы: xls, xlsx, pdf и html.

В консоли должна быть предусмотрена возможность выгрузки карточки события и сохраненной теневой копии файлов.

В консоли должна быть предусмотрена возможность управления доступа к шаблонам поиска событий и отчетам.

В консоли должна быть защита от простого создания пароля и перебора пароля.

В консоли должен вестись подробный журнал действий оператора параметры: поисковые запросы, старые и новые значения параметров политик при их изменении и т.д. В случае отсутствия собственной системы сбора событий, должна быть возможность передачи данных этого журнала во внешние системы сбора событий.

4.2.6 Требования к подсистеме управления клиентским программным обеспечением

Подсистема управления клиентским программным обеспечением должна предоставлять возможность удаленной установки/обновления/удаления клиентского программного обеспечения (агента) из консоли.

Подсистема управления клиентским программным обеспечением также должна предоставлять возможность создания инсталляционного пакета агента, с возможностью распространения через GPO и установки непосредственно на рабочем месте пользователя.

Подсистема управления клиентским программным обеспечением должна обеспечивать возможность обновления агентского ПО при использовании SMB и/или FTP ресурсов с целью снижения нагрузки на сетевое соединение.

Агент Системы защиты КИ должен функционировать в среде следующих операционных систем (не ограничиваясь):

Microsoft Windows 7 Service Pack 1;

Microsoft Windows 8 и 8.1;

Microsoft Windows 10;

Microsoft Windows Server 2008 R2;
Microsoft Windows Server 2012;
Microsoft Windows Server 2012 R2;
Microsoft Windows Server 2016;
Microsoft Windows Server 2019;

Агент Системы защиты КИ должен предоставлять возможность скрытой работы в системе и не должен обнаруживаться стандартными средствами.

Агент Системы защиты КИ должен использовать предварительное шифрование данных, а также использовать защищенное соединение для передачи перехваченных объектов в подсистему анализа.

Агент Системы защиты КИ должен поддерживать работоспособность в режиме SecureBoot.

4.2.7 Требования к подсистеме визуальной аналитики информационных потоков

Подсистема визуальной аналитики информационных потоков должна обрабатывать информацию из базы данных Системы защиты КИ и предоставлять доступ к этой информации в режиме реального времени без постоянных обращений к базе Системы защиты КИ.

Сервер подсистемы визуальной аналитики должен поддерживать установку на любую из указанных операционных систем (не ограничиваясь):

Linux;
Red Hat Enterprise Linux;
CentOS Linux;
Oracle Linux и/или др.

Сервер подсистемы визуальной аналитики информационных потоков должен поддерживать использование СУБД PostgreSQL, Oracle, Mongo DB, My SQL и/или др.;

Доступ к консоли пользователя должен осуществляться через веб-интерфейс и/или графического интерфейса. Подсистема визуальной аналитики информационных потоков должна обеспечивать:

- формирование динамической сводки безопасности по филиалам организации, создание единого центра статистики и управления инцидентами;
- формирование динамической сводки безопасности по всей организации или по отделам с возможностью перестраивать сводку по новым срезам данных в режиме реального времени;
- построение интерактивного графа связи для анализа связей сотрудников внутри организации и с внешними контактами. Узлы и связи на графе должны быть интерактивными (с возможностью посмотреть детализацию по событиям и сотрудникам), а также поддерживаться фильтрация по e-mail адресам или доменам получателей, категории информации с произвольной требуемой комбинацией признаков и пр. параметрам;
- отображение всех событий от всех пользователей на одном графе связей в режиме «по умолчанию» без необходимости добавления интересуемых пользователей к графу связей;
- построение маршрута перемещения для выбранного типа информации или определенных файлов. Должна быть возможность выбрать определенный тип информации или указать список файлов и отобразить на графе всех сотрудников, которые обменивались данной информацией в указанный период времени;
- формирование интерактивного досье на сотрудника организации или любой внешний контакт с отображением детализации по событиям, а также построение индивидуального графа связи и дополнение комментариями и файлами;
- отображение ресурсов с наибольшим трафиком по количеству событий;

- организация доступа к деталям отображаемой информации на основании ролевой модели;
- отображение отправки сообщений самому себе на личную почту в виде кольцевых связей, фильтрацию данных по количеству получателей, использованию публичной почты;
- возможность изменения фильтра отображаемых данных без составления запросов, а выбором элемента кликом мыши на любой диаграмме;
- сохранение выявленных аномалий и комментариев офицера безопасности в поведении сотрудника в рамках досье;
- мониторинг состояния системы для проведения диагностики.

4.3 Перспективы развития и модернизации Системы защиты КИ

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

Система защиты КИ должна допускать расширение функциональных возможностей за счет дополнительных модулей, требования к которым описаны ниже. Описанные модули не должны требовать дополнительной разработки со стороны производителя программного обеспечения, используемого при построении Системы защиты КИ.

Модуль лингвистического анализа должен обеспечивать возможность установки дополнительных классификаторов с поддержкой, как минимум, следующих языков: русский, английский, немецкий, французский, испанский, итальянский, арабский, украинский, азербайджанский, турецкий, казахский, узбекский, армянский, чешский, таджикский, киргизский, китайский, японский.

Система защиты КИ должна обеспечивать возможности мониторинга, анализа, а также оценки эффективности работы сотрудников: перехват и хранение информации снимков экранов с настраиваемой периодичностью; возможность категоризации посещенных сайтов, запускаемых приложений; мониторинг и отображение отчетов по активности пользователя в течение заданного периода: мониторинг программ и сайтов, поисковых запросов, времени работы пользователя (вход в систему, выход из системы, активность/простой рабочей станции), создание индивидуального графика работы для каждого сотрудника, отделов.

Система защиты КИ должна обеспечивать возможность интеграции с внешними системами за счёт использования различных API (программных интерфейсов приложения), функционал которых описан ниже.

API, применяемого для получения данных из сторонних систем (с возможностью обогащения событий новыми атрибутами, используемыми подсистемами анализа и применения политик) перехвата информации с различных каналов, для последующего анализа перехваченной информации средствами Системы защиты КИ.

Система защиты КИ должна предоставлять возможность интеграции с системами класса SIEM (MaxPatrol, Комрад, NeuroDAT SIEM, ArcSight ESM, QRadar и/или др.) для отправки событий из Системы защиты КИ в системы класса SIEM.

Система защиты КИ должна обеспечивать возможность интеграции с решениями Check Point без установки дополнительного аппаратного и программного обеспечения, с возможностью расшифровки HTTPS трафика, с передачей авторизационных данных пользователя (учётная запись) и IP адреса компьютера.

4.4 Требования к техническому обеспечению

Необходимые вычислительные ресурсы необходимые для функционирования поставляемого решения будут предоставлены силами и средствами Заказчика. При этом, Исполнитель должен предоставить информацию о вычислительных ресурсах, необходимых для полноценного функционирования информационной системы без привязки к продукциям определенного производителя.

5 Требования к проведению работ

Основные решаемые задачи:

анализ документов Заказчика, регламентирующих работу с конфиденциальной информацией, и организационно-штатной структуры Заказчика;

разработка защищаемых данных с помощью элементов технологий анализа в Системе защиты КИ для выявления в документах конфиденциальной информации;

идентификация путей перемещения и мест хранения КИ, сбор и анализ информации для разработки и настройки политик реакции Системы защиты КИ;

внедрение Системы защиты КИ.

До начала выполнения работ Заказчик и Исполнитель должны:

назначить Ответственного представителя (от Заказчика) и Руководителя работ (от Исполнителя), которые уполномочены оперативно решать все организационные и технические вопросы при выполнении и сдаче-приемке выполненных работ;

подписать соглашение о неразглашении конфиденциальной информации;

перед началом очередной стадии работ по проекту согласовать детальный график работ;

согласовать порядок входа на объект и режим пребывания специалистов Исполнителя на объекте в течение рабочего дня, а при необходимости, также в вечернее время и в выходные дни;

для своевременного контроля над ходом проведения работ согласовать порядок предоставления Заказчику отчетов о выполненных и проводимых работах;

согласовать порядок сдачи выполненных монтажных работ и проведения приемо-сдаточных испытаний.

5.1 Требования к месту проведения работ

Исполнитель должен выполнить поставку лицензий и пусконаладку по следующему адресу - Узбекистан, 100017, г. Ташкент, Юнусабадский р-н, ул. Истиклол, 29.

5.2 Требования к подготовке исходных данных

Для реализации работ Заказчик должен предоставить Исполнителю все необходимые для проведения работ исходные данные, в том числе:

документы, содержащие конфиденциальную информацию, и организационно-штатную структуру;

пути перемещения и места хранения КИ;

информацию о серверах и рабочих станциях, функционирующих инфраструктуре Заказчика;

информацию о существующей системе управления настройками серверов и рабочих станций и правами пользователей.

Получение любой информации от работников Заказчика, необходимой для выполнения проекта, должно осуществляться Исполнителем в режиме интервьюирования, заполнения опросных листов, по электронной почте.

Перечень исходных данных может уточняться и дополняться в ходе выполнения работ установленным порядком.

5.3 Требования к последовательности проведения работ, этапам работ

Работы должны быть проведены в несколько основных этапов в следующем порядке:

Обследование документов Заказчика, содержащих КИ, формирование классификатора и политик Системы защиты КИ.

3) Проектирование Системы защиты КИ.
4) Пусконаладочные работы. Установка и настройка Системы защиты КИ.

5) Опытная эксплуатация.
6) Приемочные испытания и ввод системы в промышленную эксплуатацию.

Сроки выполнения этапов работ должны найти свое отражение в коммерческом предложении Исполнителя. При этом, общий срок внедрения системы не должно превышать 90 рабочих дней.

Приемка системы будет осуществляться по мере выполнения работ по каждому из этапов. По факту выполнения каждого из этапов будет подписан акт выполненных работ.

5.4 Требования к оформлению документов, предоставляемых в ходе оказания услуг

В рамках реализации проекта Исполнитель должен подготовить следующие документы, которые делятся на два вида:

Рабочая документация на Систему защиты КИ:

1)Техническое задание;

2)Программа и методика испытаний.

Эксплуатационная документация на Систему защиты КИ:

3)Руководство пользователя;

4)Руководство администратора.

Отчетные материалы предоставляются Исполнителем в 2-х экземплярах в бумажном и электронном виде. При передаче информации в электронном виде используется формат Microdoft Word (*.doc). Вместе с программным обеспечением предоставляются относящиеся к нему документы, оформленные надлежащим образом.

5.5 Порядок предъявления и согласования результатов работ

Работы принимаются Заказчиком в соответствии с требованием настоящего технического задания.

Все проекты разработанных Исполнителем документов должны быть переданы на согласование в ответственные подразделения Заказчика.

Заказчик организует процесс согласования переданных проектов документов. Срок согласования представленных Исполнителем документов составляет не более десяти рабочих дней и не входит в срок выполнения работ.

5.6 Требования к обучению персонала

Исполнитель должен осуществить обучение персонала Заказчика по установке, настройке и эксплуатацию программного обеспечения

5.7 Требования к техническому сопровождению

Исполнитель должен обеспечить техническое сопровождение в течении 1 года с момента запуска системы в эксплуатацию и подписания Заказчиком акта ввода в эксплуатацию.