ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку лицензий автоматизированной системы обнаружения и фильтрации контента

Москва 2020 год

Содержание

1 Общие требования

1.1 Полное наименование поставки

Поставка лицензий на Автоматизированную систему обнаружения и фильтрации контента (далее Система ОФК) в АНО «РСИ» (далее Заказчик).

В рамках поставки лицензий Заказчику должен предоставляться набор ПО в виде дистрибутива для установки сервера приложений и базы данных Системы ОФК.

1.2 Назначение Системы ОФК

Система ОФК предназначена для автоматизации деятельности персонала Заказчика, направленной на обеспечение информационной безопасности, в части обнаружения и реагирования на события, возникающие в процессе обработки, хранения и перемещения информации.

1.3 Сроки поставки лицензий

Сроки поставки лицензий Системы ОФК в течении 10 календарных дней с момента заключения договора между Заказчиком и Исполнителем.

2 Требования к Системе ОФК

2.1 Требования к Системе ОФК в целом

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

Система ОФК должна обеспечивать возможность контроля не менее «150» учётных записей пользователей.

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

2.1.1 Требования к способам и средствам связи для информационного обмена

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

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

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

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

2.1.2 Требования к характеристикам взаимосвязей

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

Система ОФК 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 ОФК 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.

2.1.3 Требования к режимам функционирования Системы ОФК

Система ОФК должна функционировать в автоматизированном режиме под управлением администратора.

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

2.1.4 Требования по диагностированию Системы ОФК

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

2.1.5 Требования к численности и квалификации персонала

Персонал Заказчика, ответственный за администрирование Системы ОФК, должен иметь базовые знания в области широко используемых в настоящее время в корпоративной среде информационных технологий – в том числе операционных систем АРМ и серверов, сетевых протоколов, централизованных систем идентификации и аутентификации, систем электронной почты и т.п.

2.1.6 Требования к унификации

Система ОФК должна иметь сертификат ФСТЭК России, который удостоверяет соответствие требованиям, обозначенным в:

- руководящем документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) по 5 классу защищенности;
- документах «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) и «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4. ПЗ» (ФСТЭК России, 2014).

Сведения о Системе ОФК должны быть включены в «Единый реестр российских программ для электронных вычислительных машин и баз данных».

Требования к унификации не распространяются на подсистему визуальной аналитики информационных потоков Системы ОФК.

2.1.7 Требования к надежности

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

Система ОФК 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 ОФК.

2.2 Требования к функциональным возможностям Системы ОФК

2.2.1 Требования к подсистеме перехвата трафика

Подсистема перехвата трафика должна обеспечивать перехват и обработку трафика в т.ч. контроль терминальных клиентов, подключенных к терминальному серверу посредством Microsoft RDP или Citrix ICA.

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

Подсистема перехвата трафика должна обеспечивать контроль действий по отправке информации в ситуации, когда клиент находится вне локальной сети компании.

Подсистема перехвата трафика должна предоставлять возможности обработки следующих типов объектов:

1) распаковка архивов (7z, exe, xz, lzh, gz, bzip, bz2, tar, arj, rar, zip, zipx, cab, uha, zlib);
2) детектирование по сигнатуре:
   а) архивы (z, lzw);
   б) базы данных (ace, mdb, accdb, dmp, mxl, vcs, vcsrd, bak, trn, full, dt, cf);
   в) мультимедиа (cdr, ico, jxr, hdp, wdp, mov, ape, flac, wma, wmv, asf, mp3, wav, mpg, ogg, avi, m4a, aac, flv, mp4, 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);
   г) конструкторские файлы (CATPart, CATProduct, CATDrawing, CATProcess, CATAnalysis, CATCatalog, CATMaterial, plt, sldprt, sldasm, slddrw, prtdot, asmdot, drwdot, prt, cdw, m3d, a3d, a3t, cdt, spt, spw, frt, frw, kdt, kdw, m3t, t3d, dgn, rvt, rfa, fbx, step, stp, igs, sat);

д) исполняемые файлы и библиотеки (rpm, so, exe, dll);

е) другие файлы (xlsb, eml, der, p7s, ink, p7m, otf, torrent, gpg, pgp, gpg, asc, kdb, kdb2, wim);

3) детектирование и извлечение текста:

а) конструкторские файлы (dwg, dwt, dws);

б) презентации (ppt, pptx, pot, potm, potx, odp);

в) таблицы (xls, xlsx, xlt, xltm, xltx, ods);

г) 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);

д) почтовые сообщения (tnef, tnf, winmail.dat, msg);

е) другие файлы (odg, mpp, iso, oxps, xps);

Подсистема перехвата трафика должна выявлять факты склейки файлов и несоответствия расширения файла и его сигнатуры.

Подсистема перехвата 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.

2.2.1.1 Требования к модулю контроля корпоративной почты

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

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

Модуль должен обеспечивать возможность осуществлять разрешение или запрет для пользователей на отправку и получение почтовых сообщений по протоколам SMTP(S), POP3(S), IMAP4(S), MAPI.

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

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

Модуль должен предоставлять возможность помещения почтовых сообщений на карантин по результатам анализа содержимого, передаваемых по протоколу SMTP, без необходимости установки клиентского программного обеспечения. В случае подтверждения нарушения 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.

2.2.1.2 Требования к модулю контроля 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 выделять из веб-трафика входящие и исходящие сообщения на ресурсах vk.com и facebook.com и предоставлять возможность объединения сообщений в диалоги по заданным настройкам времени и количества сообщений.

Модуль должен обеспечивать возможность управления доступом (в том числе ограничивать доступ только на чтение) пользователей при работе с веб-клиентами облачных хранилищ (DropBox, Google Drive, Яндекс.Диск, Microsoft OneDrive, Evernote, SugarSync).

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

2.2.1.3 Требования к модулю контроля мессенджеров

Модуль должен обеспечивать перехват и обработку сообщений чатов, файлов и голосовых сообщений, 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 приложений, работающих по протоколу XMPP (Miranda, QIP, Psi, Trillian, Pidgin и др. и обеспечивать возможность осуществлять разрешение или запрет для пользователей использования приложений, работающих по протоколу XMPP.

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

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

2.2.1.4 Требования к модулю контроля 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., включая терминальные устройства), 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 формирования правил подключения к некорпоративным сетям с возможностью дать доступ на заданные сервера или предоставления временного доступа к сети интернет, если рабочая станция сотрудника находится за пределами корпоративной сети.

Модуль должен обеспечивать возможность предоставления временного доступа подключения к некорпоративным сетям или разрешения работы с периферийными устройствами с использованием кода подтверждения.

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 по результатам анализа содержимого. Модуль должен обеспечивать возможность указания разрешенных имен и идентификаторов съемных устройств, каталогов источника и приёмника копирования для контроля перемещения выбранной категории данных.

2.2.1.5 Требования к модулю контроля FTP-трафика

Модуль должен обеспечивать получение копий файлов, загруженных на FTP-ресурсы, и подготовку этих данных к дальнейшему анализу.

Модуль должен обеспечивать возможность блокировки передачи данных на FTP-ресурсы по результатам анализа содержимого.

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

Модуль должен обеспечивать возможность создания политик контроля отдельных каталогов источника и приёмника копирования с использованием анализа содержимого.

2.2.1.6 Требования к модулю контроля SMB-трафика

Модуль должен обеспечивать получение копий файлов, загруженных на общие сетевые ресурсы по протоколу SMB или полученных из них, и подготовку этих данных к дальнейшему анализу.

Модуль должен обеспечивать возможность блокировки передачи данных между защищаемым АРМ и общими сетевыми ресурсами по результатам анализа содержимого.

Модуль должен обеспечивать возможность создания политик контроля отдельных каталогов источника и приёмника копирования с использованием анализа содержимого.

2.2.1.7 Требования к модулю контроля буфера обмена

Модуль должен обеспечивать перехват и обработку копии вставленного текста из буфера обмена в приложения, в том числе приложения терминальной сессии.

2.2.1.8 Требования к модулю контроля печати документов

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

2.2.1.9 Требования к модулю контроля приложений

Модуль должен обеспечивать возможность ограничения работы пользователей с приложениями на рабочих станциях на базе чёрных или белых списков приложений, включая приложения терминальной сессии.

Модуль должен обеспечивать возможность ограничения использования буфера обмена и печати в сформированном списке приложений, включая приложения терминальной сессии.

2.2.1.10 Требования к модулю контроля 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 или Astra Linux Directory, размеры файлов и типы файлов.

Модуль должен обеспечивать сканирование файлов без установки клиентского программного обеспечения.

2.2.1.11 Требования к модулю контроля снимков экрана

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

Создание снимков экрана должно происходить с настраиваемой периодичностью, при использовании приложений из настраиваемого списка, при смене активного окна и при копировании пользователем данных в буфер обмена.

2.2.2 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 информации и уменьшения количества ложных срабатываний.

2.2.2.1 Требования к модулю 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.

2.2.2.2 Требования к модулю лингвистического анализа

Модуль должен выполнять лингвистический анализ с использованием лингвистических алгоритмов, основанных на поиске определенных терминов (слов и словосочетаний) образующих иерархический справочник категорий (классификатор), причем извлеченный текст может содержать опечатки, транслитерацию или маскировочный текст, которые должны быть в свою очередь корректно обработаны.

Модуль должен предоставлять возможность настройки алгоритма лингвистического анализа с учётом регистра символов и морфологии языковых единиц.

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

В модуле должен быть преднастроенный стандартный классификатор, содержащий категории «Управление компанией», «Конкурсная документация», «Маркетинг», «Система безопасности», «Отдел кадров», «Финансы», «Договоры и контракты» и др.

Модуль должен предусматривать наличие отраслевого классификатора, содержащего следующие категории: «Строительство».

Модуль должен предусматривать возможность настройки индивидуального классификатора.

2.2.2.3 Требования к модулю детектирования цифровых отпечатков

Модуль должен выполнять поиск фрагментов, принадлежащих к задаваемым эталонным документам, составляющим базу эталонных документов.

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

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.

2.2.2.4 Требования к модулю детектирования текстовых объектов

Модуль должен выполнять поиск тестовых объектов, соответствующих регулярным выражениям.

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

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

2.2.2.5 Требования к модулю детектирования графических объектов

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

Должна обеспечиваться поддержка графических объектов, как в виде растровой графики, так и в виде векторной графики.

Должна обеспечиваться возможность обучения модуля новым графическим объектам на основе коллекции однотипных изображений (например, водительское удостоверение).

2.2.2.6 Требования к модулю детектирования кредитных карт

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

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

2.2.2.7 Требования к модулю детектирования паспортов

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

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

2.2.2.8 Требования к модулю детектирования выгрузок из баз данных

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

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

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

2.2.2.9 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.

2.2.3 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, контактов, рабочих станций, web-ресурсов в логические периметры.

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

Подсистема применения политик должна предоставлять возможности для автоматического проставления перехваченным объектам дополнительных атрибутов (теги, уровень нарушения, вердикт) из консоли управления.

Подсистема применения политик должна предоставлять возможность для автоматического проставления статусов сотрудникам 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 ОФК.

2.2.3.1 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.

Модуль должен предоставлять возможность настройки периода сканирования измененных элементов. При сканировании измененных элементов в Системе ОФК 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.

2.2.3.2 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);
- результатов анализа перехваченных объектов от подсистемы анализа;
- форматов документов;
- статуса сотрудников;
- логического периметра.

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

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, и присваивать объекту тег, соответствующий типу сайта.

Модуль должен предоставлять возможности для передачи объектов в подсистему хранения.

2.2.4 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.

2.2.5 Требования к консоли управления

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

В консоли управления должна быть предусмотрена возможность проводить полный аудит действий.

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

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

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

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

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

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

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

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

2.2.6 Требования к подсистеме управления клиентским программным обеспечением

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

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

Агент Системы ОФК должен функционировать в среде следующих операционных систем:

- Microsoft Windows Vista Service Pack 2;
- 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;

- Astra Linux Special Edition. Релиз "Смоленск" 1.6 Update 2.

Агент Системы ОФК должен предоставлять возможность скрытой работы в системе.

Агент Системы ОФК должен использовать шифрование TLS для передачи перехваченных объектов в подсистему анализа.

Агент Системы ОФК должен использовать систему авторизации для предотвращения возможности подключения к подложному центральному серверу.

Агент Системы ОФК должен поддерживать работоспособность в режиме SecureBoot.

2.2.7 Требования к подсистеме мониторинга активности пользователей

Подсистема мониторинга активности пользователей должна являться средством мониторинга, анализа, а также оценки эффективности работы сотрудников; локального проведения расследования инцидентов.

Подсистема мониторинга активности пользователей должна обеспечивать:

- получение информации о деятельности сотрудника в реальном времени:
  ж) просмотр общих сведений о рабочих станциях;
  з) просмотр запущенных процессов и открытых окон на рабочих станциях;
  и) просмотр изображений экранов;
  к) онлайн-наблюдение с экранов/веб-камер/микрофонов;
- взаимодействие с подконтрольными рабочими станциями в реальном времени:
  а) перезагрузка/выключение рабочей станции;
  б) выполнение команды;
  в) запрос лога клиента;
  г) обновление/удаление клиентского ПО;
  д) удаление локальной базы данных на компьютерах пользователей;
- взаимодействие с подконтрольными пользователями в реальном времени:
  а) завершение/блокировка сеанса (с возможностью вывода сообщения пользователю);
  б) запуск программы;
  в) запрос текущих настроек;
- перехват и хранение информации снимков экранов/веб-камер и устройств аудиозаписи (без записи тишины), с настраиваемой периодичностью;
- создание снимков веб-камер при входе или выходе пользователя из системы;
- постоянная запись информации с устройства аудиозаписи и снимков экранов с сохранением в шифрованном виде на АРМ контролируемого пользователя;

- перехват нажатий клавиш с клавиатуры на рабочем месте, отображение вводимого текста в отчетах по программам и сайтам; анализ динамики, скорости ввода текста, корректировок для формирования клавиатурного почерка пользователя;
- возможность категоризации посещенных сайтов, запускаемых приложений, вводимого текста на тематические группы, используя локальный классификатор;
- перехват текстовой информации и снимков экрана в буфере обмена;
- мониторинг отправки файлов через сайты-файлообменники (depositfiles.com, files.mail.ru и пр.) и сайты почтовых систем (mail.ru, gmail.com и пр.);
- мониторинг отправки файлов через почтовые программы (Outlook, Mail, Bat, LotusNotes, Thunderbird);
- мониторинг отправки файлов в чатах Skype, Telegram, WhatsApp, Trillian, Viber, ICQ, Mail.ru Agent, QIP, Lync, Microsoft Teams;
- перехват работы пользователей в чатах Lync, Skype, Skype Web, Viber, Telegram Desktop, Bitrix Web, Bitrix Desktop, ICQ, Mail.ru Agent, Microsoft Teams Desktop, Microsoft Teams Web;
- мониторинг и отображение отчетов по активности пользователя в течение заданного периода: мониторинг программ и сайтов, чатов/звонков, поисковых запросов, файловых операций, времени работы пользователя (вход в систему, выход из системы, активность/простой рабочей станции), интеграция с календарем Outlook и с данными СКУД Sigur;
- мониторинг устанавливаемого программного обеспечения и изменений в составе оборудования рабочей станции;
- мониторинг использования CPU/GPU;
- перехват GPS данных с построением визуального маршрута для контролируемых ноутбуков;
- отправка уведомлений о важных событиях в Telegram-чат;
- запрет доступа к веб-сайтам по настраиваемому списку;
- запрет запуска приложений согласно черным/белым спискам;
- запрет сетевых подключений через WiFi/Bluetooth/USB-модем;
- запрет использования FTP/FTPS и SSH;
- запрет буфера обмена при активном сеансе RemoteDesktop;
- запрет записи/сохранения/копирования данных на flash-диски;
- для устройств на базе Android осуществление перехвата голосовых разговоров, SMS сообщений, вводимого текста с виртуальной клавиатуры, GPS данных с

построением визуального маршрута, а также мониторинг и отображение отчетов по активности пользователя в течение заданного периода: мониторинг программ и сайтов, поисковых запросов.

2.3 Перспективы развития и модернизации Системы ОФК

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

Система ОФК 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 ОФК.

Модуль лингвистического анализа должен обеспечивать возможность установки дополнительных классификаторов с поддержкой следующих языков: немецкий, французский, испанский, итальянский, арабский, украинский, румынский (молдавский), латышский, польский, азербайджанский, турецкий, сербский, казахский, малайский, голландский, вьетнамский, португальский, узбекский, татарский, греческий, литовский, грузинский, армянский, чешский, словацкий, фарси (персидский), хинди, сингальский, таджикский, якутский, киргизский, китайский.

Система ОФК 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. Наличие интеграции между поставляемым ПО и оборудованием Check Point должно подтверждаться официальным письмом от производителя Check Point с предоставлением результатов проведения успешного тестирования.

Система ОФК должна обеспечивать возможность интеграции с решением Ethersensor для обеспечения перехвата HTTP, SMTP, POP3, IMAP4, OSCAR, FTP, SMB/CIFS, Skype, WebSocket, WebDAV и др. на скорости до 20 Гбит/с без установки агентов Системы ОФК.

Система должна обеспечивать возможность интеграции с решением SAP ERP 6.0 с целью выгрузки защищаемых объектов из данной системы и автоматической актуализации защищаемых данных. Используемые при этом Add-on должны быть сертифицированы согласно процедурам производителя данной системы, должны иметь возможности по установки правил выгрузки (периодичность, объем) и отображения статусов выгрузок и журнал выполнения.

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

Система ОФК должна обеспечивать возможность интеграции с сервисом обмена мгновенными сообщениями Cisco UCM для перехвата и обработки сообщений чатов и файлов, отправленных при помощи этого сервиса.

Система ОФК должна обеспечивать возможность интеграции с решениями ЦРТ Smart Logger II (для контроля голосовых телефонных звонков пользователей при использовании корпоративной АТС и VoIP решений) и Незабудка (пассивная запись аналоговых источников и цифровой телефонии по протоколам ISDN).

Система ОФК должна обеспечивать возможность интеграции с сервисом обмена мгновенными сообщениями Microsoft Lync для перехвата и обработки сообщений чатов, протоколирования передачи файлов и совершения голосовых вызовов, совершённых при помощи этого сервиса.

Система ОФК должна обеспечивать возможность интеграции с почтовым сервером на базе Lotus Domino для перехвата почтовых сообщений по протоколу NRPC.

Система ОФК должна обеспечивать возможность интеграции с решением WorksPad для контроля работы пользователей с корпоративной почтой и документами на мобильных устройствах на базе iOS и Android.

Система ОФК должна обеспечивать возможность интеграции с системой печати DPrint для перехвата событий печати.

Система ОФК должна обеспечивать возможность интеграции с внешними системами за счёт использования различных API (программных интерфейсов приложения):

- API, применяемого для получения данных из сторонних систем перехвата информации (с возможностью обогащения событий новыми атрибутами, используемыми подсистемами анализа и применения политик) с различных каналов, для последующего анализа перехваченной информации средствами Системы ОФК;
- API, применяемого для автоматической загрузки «Эталонных выгрузок баз данных» и «базы цифровых отпечатков» из сторонних систем;
- API, применяемого для отправки содержимого и метаданных событий из Системы ОФК в различные сторонние системы.

Система ОФК должна обеспечивать возможность интеграции с решением R-Vision IRP для отправки событий из Системы ОФК в R-Vision IRP для последующего анализа и

хранения всех инцидентов информационной безопасности в единой информационной системе.

Система ОФК должна обеспечивать возможность интеграции с корпоративным облачным хранилищем на базе Mflash для анализа событий, происходящих в MFlash средствами Системы ОФК.

Система ОФК должна обеспечивать возможность интеграции с системой повышения уровня осведомленности пользователей Awareness Center для отправки событий из Системы ОФК в Awareness Center для обучения правилам обращения с информационными активами организации сотрудников, которые неумышленно их нарушают.