Приложение № 1
к Извещению о проведении закупки
способом открытого запроса цен

Техническое задание

На приобретение лицензий программного обеспечения и оказание услуг по внедрению автоматизированной системы защиты конфиденциальной информации

Содержание

1. Перечень сокращений

BIN	Bank Identification Number. Банковский идентификационный номер
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.
DLP	Data Loss Prevention. Система предотвращения утечек 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.
FTP	File Transfer Protocol. Протокол передачи файлов по сети.
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.
MIME	Multipurpose Internet Mail Extensions. Расширения почтовых сообщений
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.
OCR	Optical Character Recognition. Оптическое распознавание символов.
OLAP	Online Analytical Processing. Онлайн-аналитическая обработка
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.
RDP	Remote Desktop Protocol. Протокол удалённого рабочего стола
SIEM	Security Information and Event Management. Система управления событиями ИБ
SMB	Server Message Block. Сетевой протокол для удаленного доступа к файлам и принтерам.
SMTP(S)	Simple Mail Transfer Protocol. Широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.
SSL	Secure Sockets Layer. Криптографический протокол безопасности
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.
XMPP	eXtensible Messaging and Presence Protocol. Открытый, свободный для использования протокол мгновенного обмена сообщениями и информацией о присутствии в режиме, близком к режиму реального времени.
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИНН	Идентификационный номер налогоплательщика
КИ	Конфиденциальная информация
КПП	Код причины постановки на учёт в Федеральную Налоговую Службу
ПК	Персональный компьютер
ПО	Программное обеспечение
СНИЛС	Страховой номер индивидуального лицевого счёта
СКУД	Система контроля и управления доступом
СУБД	Система управления базами данных
ФСТЭК	Федеральная Служба по Техническому и Экспортному Контролю

2. Общие требования

2.1 Цель задания

Поставка всех необходимых лицензий и внедрение автоматизированной системы защиты конфиденциальной информации (далее Система защиты КИ) для Евразийского фонда стабилизации и развития (далее Заказчик).

2.2 Назначение Системы защиты КИ

Система защиты КИ предназначена для автоматизации деятельности сотрудников 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;

- мониторинга действий сотрудников и защиты от внутренних угроз (в т.ч. фиксация несанкционированного доступа, использования запрещенных ресурсов, аномального поведения), контроля соблюдения политик безопасности, целевого использования корпоративных ресурсов.

2.3 Сведения об инфраструктуре Заказчика

2.3.1 Вычислительная инфраструктура

Серверная инфраструктура представляет собой 2 гео-распределенных ЦОДа, находящихся под управлением платформы виртуализации VMware vSphere.

Вычислительные ресурсы (vCPU, RAM, диск) под компоненты Системы защиты КИ будут выделены из пула инфраструктуры Заказчика.

В инфраструктуре используется Microsoft Exchange Server, развернутый локально.

2.3.2 Сетевая инфраструктура

Пользователи в центральном офисе, а также удаленных офисов, подключаются к инфраструктуре по VPN каналу до инфраструктуры. Удаленные пользователи подключаются до инфраструктуры посредством VPN. Общее количество пользователей на текущий момент - 140 человек.

2.4 Сроки поставки лицензий и внедрения, информация об условиях договора.

Сроки поставки лицензий и внедрения Системы защиты КИ не должен превышать 3 месяца с даты заключения договора.

Информация об условиях договора:

- Форма оплаты – безналичный расчет;
- Порядок оплаты – постоплата, на основании акта оказанных услуг, после завершения всех этапов внедрения;
- Наличие аванса – без авансирования;
- Валюта оплаты – российские рубли (RUB);
- Срок действия договора – до 31.12.2025.

2.5 Требования к поставке лицензий на Систему защиты КИ

В рамках поставки лицензий Заказчику должно быть предоставлено:

1) Право на использование Системы защиты КИ (бессрочно) — в объеме, необходимом для выполнения задач, указанных в техническом задании.
2) Право на получение всех новых версий ПО, выпускаемых производителем в течение 1 года, включая все обновления, модификации и усовершенствования, вне зависимости от их характера (обновление безопасности, функциональное расширение, оптимизация и т.п.).
3) Право на получение уведомлений о выходе новых версий, обновлений и иной сопутствующей информации, касающейся предоставленного ПО, сроком на 1 год.
4) Техническая поддержка сроком 1 год, включающая в себя:

- консультирование по вопросам установки, настройки и эксплуатации ПО;
- устранение сбоев и ошибок в работе программного обеспечения;
- предоставление исправлений, патчей и обновлений;
- помощь в диагностике и анализе инцидентов, возникающих при использовании ПО;
- сопровождение при переходе на новые версии ПО, в том числе рекомендации по миграции данных, настройке и совместимости.

Заказчику должна предоставляться возможность дистанционного обучения основам использования Системы защиты КИ, где будет представлена информация по архитектуре решения, настройке, возможностям и принципам работы.

2.6 Порядок внедрения Системы защиты КИ

В рамках внедрения Системы защиты КИ Исполнитель должен выполнить следующие работы (этапы):

1) Обследование текущей инфраструктуры, сбор информации об используемых каналах передачи данных, действующих политиках безопасности, пользовательской активности, определение требований к настройке системы (с результатом в виде отчета в электронном формате);

2) Разработка технического задания на внедрение (с результатом в виде документа в электронном формате);
3) Разработка концепции настройки политик (с результатом в виде документа в электронном формате);
4) Разработка паспорта Системы защиты КИ (с результатом в виде документа в электронном формате);
5) Разработка программы и методики испытаний (с результатом в виде документа в электронном формате);
6) Разработка руководства администратора (с результатом в виде документа в электронном формате);
7) Установка и настройка Системы защиты КИ;
8) Инструктаж Заказчика и демонстрация Системы защиты КИ;
9) Опытная эксплуатация (сроком не более 1 мес.). В процессе и по результатам опытной эксплуатации Исполнитель должен всецело оказывать содействие и техническую поддержку по первому требованию заказчика для запуска системы в промышленную эксплуатацию;
10) Сдача-приемка Системы защиты КИ.

Выполнение каждого этапа подтверждается Заказчиком по электронной почте. Работы могут выполняться параллельно.

Факт выполнения задания Исполнителем и принятия результатов Заказчиком будет подтверждаться подписанием Акта выполненных работ.

В процессе выполнения задания Исполнитель должен взаимодействовать с Заказчиком. При возникновении вопросов, связанных с выполнением задания, Исполнитель должен обратиться к Заказчику за необходимыми уточнениями.

3. Требования к Системе защиты КИ

3.1 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 следующего количества учётных записей пользователей:

Кол-во	Название модуля/подсистемы	Выполнение требования (соответствует/не соответствует)
	Подсистема перехвата:	
140	Компонент контроля корпоративной почты: - для протокола SMTP - для протокола POP3 - для протокола IMAP4 - для протокола MAPI	соответствует
140	Компонент контроля web-трафика	соответствует
140	Компонент контроля web облачных хранилищ	соответствует
140	Компонент контроля desktop облачных хранилищ: - Microsoft OneDrive - Google Drive - Яндекс Диск - Mega - NextCloud	соответствует
140	Компонент контроля мессенджеров: - для Telegram - для XMPP (Jabber) - для социальных сетей - для WhatsApp - для eXpress	соответствует
140	Компонент контроля терминальных сессий	соответствует
140	Компонент контроля подключаемых устройств	соответствует
140	Компонент контроля FTP-трафика	соответствует
140	Компонент контроля SMB-трафика	соответствует
140	Компонент контроля вводимого текста	соответствует
140	Компонент контроля буфера обмена	соответствует
140	Компонент контроля печати документов	соответствует
140	Компонент контроля снимков экрана	соответствует
140	Компонент контроля приложений	соответствует
140	Компонент контроля файловых операций для приложений: - для Google Chrome - для Microsoft Internet Explorer - для Microsoft Edge - для Mozilla Firefox - для Яндекс Браузер	соответствует

	- для Zoom - для WhatsApp - для Viber - для Telegram	
	Подсистема анализа:	
140	Компонент OCR	соответствует
140	Компонент лингвистического анализа	соответствует
140	Компонент анализа цифровых отпечатков	соответствует
140	Компонент анализа векторных цифровых отпечатков	соответствует
140	Компонент анализа текстовых объектов	соответствует
140	Компонент анализа бланков	соответствует
140	Компонент анализа выгрузок из баз данных	соответствует
140	Компонент анализа графических объектов	соответствует
140	Компонент анализа изображений паспортов	соответствует
140	Компонент анализа изображений кредитных карт	соответствует
140	Компонент анализа печатей	соответствует
140	Подсистема мониторинга прав доступа к данным	соответствует
140	Подсистема мониторинга файловых хранилищ	соответствует
140	Подсистема визуальной аналитики информационных потоков	соответствует
140	Подсистема мониторинга активности пользователей	соответствует
140	Подсистема предиктивной аналитики	соответствует
140	Адаптер интеграции с MFlash	соответствует

Требование	Выполнение требования (соответствует/не соответствует)
Система защиты КИ должна иметь консоль проведения расследований и предоставления отчётности на русском языке через web-интерфейс.	соответствует

3.1.1 Требования к способам и средствам связи для информационного обмена

Требование	Выполнение требования (соответствует/не соответствует)
Система защиты КИ должна функционировать в составе информационно-вычислительной сети Заказчика.	соответствует
Для информационного обмена между компонентами Системы защиты КИ должны использоваться только стандартные унифицированные протоколы семейства TCP/IP.	соответствует
Система защиты КИ должна поддерживать работу в сетях, работающих по протоколам IPv4 и IPv6.	соответствует
Система защиты КИ должна обеспечивать управление загрузкой канала связи при взаимодействии с модулями, расположенными в удаленных элементах информационной системы.	соответствует

3.1.2 Требования к характеристикам взаимосвязей

Требование	Выполнение требования (соответствует/не соответствует)
Система защиты КИ должна обеспечивать возможность интеграции и идентификации объектов с данными, полученными из Active Directory, в том числе из нескольких LDAP доменов.	соответствует
Система защиты КИ должна обеспечивать возможность интеграции со следующими proxy-серверами: FortiGate и другими proxy-серверами с поддержкой ICAP.	соответствует
Система защиты КИ должна обеспечивать возможность интеграции с корпоративным файлообменным сервисом MFlash для получения теневых копий файлов и блокирования загрузки файлов по результатам контекстного анализа.	соответствует

3.1.3 Требования к режимам функционирования Системы защиты КИ

Требование	Выполнение требования (соответствует/не соответствует)
Система защиты КИ должна функционировать в автоматизированном режиме под управлением администратора.	соответствует
Система защиты КИ должна обеспечивать возможность работы в следующих режимах: штатный режим – непрерывная круглосуточная работа; сервисный режим – для проведения обслуживания, реконфигурации и модернизации компонента; автономный режим – в случае отсутствия связи между компонентами Системы защиты КИ или с внешними сетями, для доступа к конфигурационной и архивной информации.	соответствует

3.1.4 Требования по диагностированию Системы защиты КИ

Требование	Выполнение требования (соответствует/не соответствует)
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.	соответствует
Система защиты КИ должна обеспечивать возможность контроля целостности системных файлов, как в автоматическом, так и в ручном режиме.	соответствует

3.1.5 Требования к унификации

Требование	Выполнение требования

	(соответствует/не соответствует)
Система защиты КИ должна иметь сертификат ФСТЭК России, который удостоверяет соответствие требованиям, обозначенным в: Документах «Требования к средствам контроля съемных машинных носителей информации» и «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты ИТ.СКН.П4.ПЗ»; Документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» по 4 уровню доверия; Руководящем документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 5 классу защищенности».	соответствует
Сведения о Системе защиты КИ должны быть включены в «Единый реестр российских программ для электронных вычислительных машин и баз данных».	соответствует

Требования к унификации не распространяются на подсистемы визуальной аналитики информационных потоков, мониторинга активности пользователей Системы защиты КИ.

3.1.6 Требования к надежности

Требование	Выполнение требования (соответствует/не соответствует)
Система защиты КИ должна обеспечивать штатное функционирование в случае одновременной работы всех пользователей Заказчика на объекте автоматизации.	соответствует
Система защиты КИ должна обеспечивать возможность масштабирования и отказоустойчивости, в том числе поддерживать кластерные технологии.	соответствует
Должно осуществляться резервное копирование и хранение резервных копий данных, с возможностью их восстановления.	соответствует
Должна быть обеспечена непрерывность бизнес-процессов Заказчика в случае отказов Системы защиты КИ.	соответствует

3.2 Требования к функциональным возможностям Системы защиты КИ

3.2.1 Требования к подсистеме перехвата трафика

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема перехвата трафика должна обеспечивать контроль действий по отправке информации в ситуации, когда клиент находится вне локальной сети организации. Подсистема перехвата	соответствует

трафика должна извлекать из перехваченных объектов текстовую информацию и вложения, выполнять определение форматов вложений и передачу извлеченных данных в подсистему анализа.	
При возможности создания теневой копии отправленных и полученных файлов должна обеспечиваться настройка сохранения теневой копии с указанием размера и формата файла.	соответствует
Подсистема перехвата трафика должна выполнять выделение транспортных атрибутов (отправитель, список получателей) из перехваченных данных.	соответствует

3.2.1.1 Требования к компоненту контроля корпоративной почты

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать: контроль обмена данными по протоколам POP3(S), IMAP4(S), SMTP(S) (в т.ч. запрет использования протокола), создание теневых копий передаваемых файлов (при наличии), подготовку данных к дальнейшему анализу (контекст и контент).	соответствует
Компонент должен обеспечивать возможность блокировки отправки почтовых сообщений по протоколу MAPI (в т.ч. по результатам анализа содержимого). Компонент должен расшифровывать сообщения, сформированные по стандарту S/MIME, если для передачи используется протокол MAPI и криптографический провайдер Microsoft.	соответствует
Компонент должен обеспечивать возможность блокировки отправки и/или помещения на карантин почтовых сообщений по протоколу SMTP(S), в т.ч. по результатам анализа содержимого без необходимости установки клиентского программного обеспечения. В случае использования режима «карантин» при подтверждении нарушения офицером безопасности сообщения должны блокироваться, в противном случае – отправляться адресату.	соответствует
Перехват данных, передаваемых из корпоративной сети по протоколам POP3(S), IMAP4(S), SMTP(S) должен быть возможен без установки клиентского программного обеспечения.	соответствует
Система защиты КИ должна обеспечивать возможность контроля и анализа почты, которая синхронизируется между почтовым сервером и клиентским устройством по протоколам ActiveSync и IMAP.	соответствует

3.2.1.2 Требования к компоненту контроля web-трафика

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать перехват загружаемых данных по протоколам HTTP(S) (web-почта, форумы, блоги, чаты и т.д.).	соответствует

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

3.2.1.3 Требования к компоненту контроля облачных хранилищ

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать возможность управления доступом (полный доступ, только чтение, блокировка доступа) пользователей при работе с веб-клиентами облачных хранилищ: DropBox, Evernote, Google Drive, Microsoft OneDrive, Яндекс.Диск, Mflash.	соответствует
Компонент должен обеспечивать возможность перехвата файлов, который пользователь получает или отправляет другим адресатам при использовании desktop приложения сервиса: Microsoft OneDrive Google Drive Mega Яндекс Диск NextCloud Mflash	соответствует
В момент перехвата теневой копии файла должен создаваться скриншот экрана.	соответствует

3.2.1.4 Требования к компоненту контроля терминальных сессий

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать перехват и обработку трафика терминальных клиентов, подключенных к терминальному серверу посредством Microsoft RDP с возможностью определения конечного приемника при передаче файлов.	соответствует

3.2.1.5 Требования к компоненту контроля подключаемых устройств

Требование	Выполнение требования (соответствует/не соответствует)
Компонент 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.	соответствует

Компонент должен обеспечивать возможность создания белых списков устройств, доступ к которым разрешен.	соответствует
Компонент 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.	соответствует
Компонент должен обеспечивать возможность предоставления временного доступа подключения к некорпоративным сетям или разрешения работы с периферийными устройствами с использованием кода подтверждения.	соответствует
Компонент должен обеспечивать возможность запрета создания снимков экрана на рабочей станции пользователя, если снимки создаются стандартными средствами операционной системы.	соответствует
Компонент 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.	соответствует
Компонент должен обеспечивать перехват и блокировку при копировании данных с съемного устройства на АРМ и возможность указания разрешенных имен и идентификаторов съемных устройств, каталогов источника и приёмника копирования для контроля перемещения выбранной категории данных.	соответствует

3.2.1.6 Требования к компоненту контроля FTP-трафика

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать:	
контроль обмена данными по протоколу FTP(S) (в т.ч. запрет использования протокола);	соответствует
возможность создания политик для заданных каталогов источника и приёмника копирования;	соответствует
создание теневых копий передаваемых файлов (при скачивании и загрузке);	соответствует
подготовку данных к контекстному и контентному анализу;	соответствует
блокировку при передаче.	соответствует
Блокировка осуществляется по результатам контекстного анализа и анализа содержимого, в т.ч. автономном режиме (при отсутствии подключения к серверной части Системы защиты КИ) согласно политикам, сохранённым локально на защищаемом АРМ.	соответствует

3.2.1.7 Требования к компоненту контроля SMB-трафика

Требование	Выполнение требования (соответствует/не соответствует)

Компонент должен обеспечивать:	
контроль обмена данными по протоколу SMB (в т.ч. запрет передачи данных по нему);	соответствует
возможность создания политик для заданных каталогов источника и приёмника копирования;	соответствует
создание теневых копий передаваемых файлов (скачивание и загрузка);	соответствует
подготовку данных к дальнейшему анализу (контекст и контент);	соответствует
блокировку при передаче.	соответствует
Блокировка осуществляется по результатам контекстного анализа и анализа содержимого, в т.ч. в автономном режиме (при отсутствии подключения к серверной части Системы защиты КИ) согласно политикам, сохранённым локально на защищаемом АРМ.	соответствует

3.2.1.8 Требования к компоненту контроля файловых операций

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать возможность перехвата файлов, который пользователь получает или отправляет другим адресатам при использовании любых веб-сервисов, в том числе и облачных, через браузеры: Google Chrome Mozilla Firefox Microsoft Edge Microsoft Internet Explorer Яндекс Браузер	соответствует
Обработка данных должна осуществляться без подмены сертификата SSL-шифрования.	соответствует
Компонент должен обеспечивать возможность перехвата файлов, который пользователь получает или отправляет другим адресатам при использовании desktop приложения сервисов: Zoom WhatsApp Viber Telegram Express В момент перехвата теневой копии файла должен создаваться скриншот экрана.	соответствует

3.2.1.9 Требования к компоненту контроля вводимого текста

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать перехват текста при вводе с клавиатуры в приложения из настраиваемого списка.	соответствует
Компонент должен обеспечивать привязку снимков экранов к событиям клавиатурного перехвата.	соответствует

3.2.1.10 Требования к компоненту контроля буфера обмена

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать перехват и блокировку операций копирования и вставки данных через буфера обмена в приложениях.	соответствует
Компонент должен обеспечивать перехват операций копирования и вставки, контентный анализ и блокировку на основании анализа данных через буфера обмена в приложениях терминальной сессии.	соответствует

3.2.1.11 Требования к компоненту контроля печати документов

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать перехват, блокировку и обработку теневых копий файлов, отправленных на печать на локальные и сетевые принтеры.	соответствует
Блокировка осуществляется по результатам контекстного анализа и анализа содержимого, в т.ч. автономном режиме (при отсутствии подключения к серверной части Системы защиты КИ) согласно политикам, сохранённым локально на защищаемом АРМ.	соответствует

3.2.1.12 Требования к компоненту контроля снимков экрана

Требование	Выполнение требования (соответствует/не соответствует)
Компонент 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.	соответствует
Компонент должен обеспечивать создание снимков экрана с рабочих станций, если активны приложения из заранее заданного списка и обеспечивать их передачу в подсистему хранения.	соответствует
Дополнительно Система защиты КИ должна обеспечивать распознавание текста на снимках экранов с рабочих станций, а также анализ полученного текста технологиями анализа с возможностью производить полнотекстовый поиск по результату.	соответствует

3.2.1.13 Требования к компоненту контроля приложений

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать возможность ограничения работы пользователей с приложениями на рабочих станциях на базе чёрных	соответствует

или белых списков приложений, включая приложения терминальной сессии.	
Компонент должен обеспечивать возможность ограничения использования буфера обмена и печати в сформированном списке приложений, включая приложения терминальной сессии.	соответствует

3.2.1.14 Требования к компоненту контроля мессенджеров

Требование	Выполнение требования (соответствует/не соответствует)
Компонент 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 приложения сервиса обмена мгновенными сообщениями Telegram.	соответствует
Компонент должен обеспечивать перехват и обработку сообщений чатов и файлов, отправленных при помощи приложений, работающих по протоколу XMPP и обеспечивать возможность осуществлять разрешение или запрет для пользователей использования приложений, работающих по протоколу XMPP.	соответствует
Компонент должен выделять из веб-трафика входящие и исходящие сообщения ресурса vk.com и предоставлять возможность объединения сообщений в диалоги по заданным настройкам времени и количества сообщений.	соответствует
Компонент должен обеспечивать перехват и обработку сообщений чатов и файлов, отправленных при помощи сервиса обмена мгновенными сообщениями Skype.	соответствует
Компонент должен обеспечивать перехват и обработку сообщений чатов и файлов, отправленных и полученных при помощи сервиса обмена мгновенными сообщениями WhatsApp и обеспечивать возможность осуществлять разрешение или запрет для пользователей использования приложения сервиса обмена мгновенными сообщениями WhatsApp.	соответствует
Система защиты КИ должна обеспечивать интеграцию с сервером платформы корпоративных коммуникаций eXpress с возможностью перехвата входящих и исходящих сообщений, перехвата теневых копий вложенных файлов, определения идентификатора отправителя и получателя и времени отправки сообщения.	соответствует

3.2.2 Требования к подсистеме анализа

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема анализа должна обеспечивать анализ всех перехваченных данных и их передачу в подсистему применения политик.	соответствует

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. Должна обеспечиваться возможность детектирования объекта защиты в конкретном элементе письма.	соответствует
Подсистема анализа должна обеспечивать возможность исключения объекта защиты при срабатывании политик безопасности. Например, в случаях, когда необходимо определять грифованную информацию по словосочетанию «Коммерческая тайна» и не срабатывать на дисклеймер в подписях писем сотрудников.	соответствует
Подсистема анализа должна предоставлять возможности обработки следующих типов объектов:	
распаковка архивов (7z, exe, xz, lzh*, gz*, bzip*, bz2*, tar*, arj*, rar*, zip*, zipx*, cab*, uha*, zlib*);	соответствует
детектирование по сигнатуре:	соответствует
архивы (z, lzw);	соответствует
базы данных (ace, mdb, accdb, dmp, mxl, vcs, vcsrd, bak, trn, full, dt, cf);	соответствует
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, WebP);	соответствует
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);	соответствует
исполняемые файлы и библиотеки (rpm, so, exe, dll);	соответствует
другие файлы (xlsb, eml, der, p7s, ink, p7m, otf, torrent, gpg, pgp, gpg, asc, kdb, kdb2, wim);	соответствует
файлы без форматов (Gerber Technology file, Vector Data);	соответствует
детектирование и извлечение текста:	соответствует
конструкторские файлы (dwg, dwt, dws);	соответствует
презентации (ppt, pptx, pot, potm, potx, odp);	соответствует
таблицы (xls, xlsx, xlt, xltm, xltx, ods);	соответствует
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*, epub*);	соответствует
почтовые сообщения (tnef*, tnf*, winmail.dat*, msg*);	соответствует
другие файлы (odg, mpp, iso, oxps, xps);	соответствует
файлы без форматов (Microsoft Compound Binary File)	соответствует
Подсистема анализа должна выявлять факты склейки файлов и несоответствия расширения файла и его сигнатуры.	соответствует
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.	соответствует

*форматы, которые Система защиты КИ должна обрабатывать при наличии программного обеспечения iFilter.

3.2.2.1 Требования к компоненту OCR

Требование	Выполнение требования (соответствует/не соответствует)
Компонент OCR (ABBYY) должен обеспечивать распознавание текста, содержащегося в изображениях, полученных от подсистемы перехвата трафика.	соответствует
Текст, распознанный модулем OCR, должен анализироваться остальными технологиями анализа.	соответствует
Компонент 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.	соответствует

3.2.2.2 Требования к компоненту лингвистического анализа

Требование	Выполнение требования (соответствует/не соответствует)
Компонент 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.	соответствует
Компонент должен предоставлять возможность настройки алгоритма лингвистического анализа с учётом регистра символов и морфологии языковых единиц.	соответствует
Компонент должен предоставлять возможность проведения лингвистического анализа для следующих языков: русский*, английский* (* - поддержка морфологии языка в дополнение к точным совпадениям с терминами соответствующего словаря).	соответствует
Должен быть преднастроенный стандартный классификатор, содержащий категории «Управление организацией», «Конкурсная документация», «Маркетинг», «Система безопасности», «Отдел кадров», «Финансы», «Договоры и контракты» и др.	соответствует
Компонент должен предусматривать наличие следующих отраслевых классификаторов: базовая.	соответствует
Компонент должен предусматривать возможность настройки индивидуального классификатора.	соответствует

3.2.2.3 Требования к компоненту анализа цифровых отпечатков

Требование	Выполнение требования (соответствует/не соответствует)

Компонент должен выполнять поиск фрагментов, принадлежащих к задаваемым эталонным документам, составляющим базу эталонных документов.	соответствует
Для добавляемых пользователем эталонных документов должен формироваться текстовый, бинарный или текстовый и бинарный отпечатки, для каждого из которых должна поддерживаться возможность указания отдельного порога цитируемости.	соответствует
Компонент должен поддерживать возможность автоматической синхронизации базы цифровых отпечаток с сетевыми каталогами.	соответствует
При обработке перехваченных событий с использованием цифровых отпечатков текстового вида, Система защиты КИ должна фиксировать факт передачи документов в виде файлов любого формата из поддерживаемых или письма (в т.ч. текстового сообщения), содержащих вставленный текст из защищаемого документа.	соответствует

3.2.2.4 Требования к компоненту анализа векторных цифровых отпечатков

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен выполнять поиск фрагментов, принадлежащих к задаваемым эталонным чертежам, составляющим базу эталонных чертежей, причем фрагменты могут быть повернуты, отмасштабированы или перенесены из одного чертежа в другой, что должно быть в свою очередь корректно обработано модулем.	соответствует
Для добавляемых пользователем эталонных документов должен формироваться векторный отпечаток, для которого должна поддерживаться возможность указания порога цитируемости.	соответствует

3.2.2.5 Требования к компоненту анализа текстовых объектов

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен выполнять поиск тестовых объектов, соответствующих регулярным выражениям.	соответствует
Компонент должен содержать предустановленные шаблоны текстовых объектов (номер паспорта гражданина Российской Федерации, 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 должны проверяться BIN номер банка и контрольная цифра).	соответствует
Компонент должен предоставлять возможность добавления текстовых объектов на основе языка регулярных выражений.	соответствует

3.2.2.6 Требования к компоненту анализа бланков

Требование	Выполнение требования

	(соответствует/не соответствует)
Компонент должен позволять отслеживать наличие заполненных и пустых эталонных бланков, анкет и формуляров как в тексте объектов, так и во вложениях.	соответствует
Компонент должен предоставлять возможность загрузки эталонных бланков для обучения модуля детектирования бланков.	соответствует
Должна быть предусмотрена возможность задать минимальное число заполненных полей для детектирования.	соответствует

3.2.2.7 Требования к компоненту анализа графических объектов

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен позволять отслеживать в поступающих на анализ изображениях наличие топографических карт, чертежей и прочих графических объектов.	соответствует
Должна обеспечиваться возможность обучения модуля новым графическим объектам на основе коллекции однотипных изображений (например, водительское удостоверение).	соответствует
Возможность обучения модуля должна обеспечиваться в рамках графического интерфейса web-консоли.	соответствует
Компонент должен обеспечивать детектирование объектов «Лица», «Технические чертежи» и «Сертификаты» без дополнительного обучения.	соответствует

3.2.2.8 Требования к компоненту анализа изображений кредитных карт

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен позволять отслеживать наличие в поступающих на анализ изображениях кредитных карт.	соответствует
Для детектирования кредитных карт не должно требоваться добавление эталонных документов в Систему защиты КИ. Изображения кредитных карт должны проходить дополнительную верификацию по наличию изображений логотипов платежных систем на карте (VISA, Visa Electron, MasterCard, Maestro, МИР).	соответствует

3.2.2.9 Требования к компоненту анализа изображений паспортов

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен позволять отслеживать наличие в поступающих на анализ изображениях главного разворота паспорта гражданина Российской Федерации.	соответствует
Для детектирования паспортов не должно требоваться добавление эталонных документов в Систему защиты КИ. Изображения	соответствует

паспортов должны проходить дополнительную верификацию по наличию изображений лица человека в месте стандартного расположения фотографии.	

3.2.2.10 Требования к компоненту анализа печатей

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен позволять отслеживать наличие эталонных печатей на изображениях отсканированных документов.	соответствует
Компонент должен предоставлять возможность загрузки эталонных изображений печати для обучения модуля детектирования печатей.	соответствует

3.2.2.11 Требования к компоненту анализа выгрузок из баз данных

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен обеспечивать детектирование в текстах и вложениях объектов выгрузок из баз данных.	соответствует
Компонент должен предоставлять возможность задания следующих условий детектирования выгрузок из баз данных: Условия совокупности столбцов, сочетание которых будет считаться конфиденциальной информацией (например, только ФИО сотрудника не будет являться таковой, а ФИО сотрудника с контактным телефоном и номером и серией паспорта будет); Задание количества строк, обнаружение которых будет детектироваться как наличие в объекте выгрузки из баз данных.	соответствует
Компонент должен обеспечивать проверку легитимности получателя, определяя кому принадлежит фрагмент выгрузки из баз данных. Идентификация должна происходить в соответствии с ключевым полем в эталонной базе данных. Ключевым полем может быть адрес электронной почты, почтовый домен, булевое значение, идентификационные данные.	соответствует
Компонент должен обеспечивать обнаружение данных, записанных в разной форме. Должно поддерживаться обнаружение таких объектов, как: номер телефона, номер банковской карты, номер банковского счета. Например, если в одном из полей указан номер телефона «79051533176», в перехваченном письме должен быть обнаружен номер телефона записанной в разной форме «+79051533176», «8(905)1533176», «8-905-153-31-76» и т.д.	соответствует

3.2.3 Требования к компоненту автоматизированного определения тематических категорий документов

Требование	Выполнение требования (соответствует/не соответствует)

Компонент должен предоставлять возможность автоматизированного определения тематических категорий (кластеров) в базе документов, перехваченных Системой защиты КИ, и распределения базы документов по кластерам. Определение тематики должно выполняться на основе результатов анализа содержимого документов без использования заданных заранее словарей и классификаторов. Распределение документов по выделенным кластерам должно выполняться определением соответствия содержимого документа наиболее близкому по тематике кластеру.	соответствует
Процесс кластеризации должен включать в себя: объединение в один кластер документов схожей тематики; выделение внутри кластера групп однотипных документов; формирование для каждого кластера облака тегов, характеризующих тематику кластера; выделение документов, наиболее релевантно отражающих тематику кластера.	соответствует
По завершению процесса кластеризации Система защиты КИ должна сформировать результаты для автоматизации создания специфического для компании словаря.	соответствует

3.2.3.1 Требования к компоненту для автоматизированного формирования специфических словарей

Требование	Выполнение требования (соответствует/не соответствует)
Компонент должен предоставлять возможность автоматизировать формирование специфических словарей путем создания индивидуального классификатора данных на основе определенной пользователем выборки документов.	соответствует
Должна быть предусмотрена возможность создания индивидуального классификатора на основе выборки документов, полученных в результате автоматизированного определения тематических категорий (кластеризации) или создания категорий документов пользователем в консоли Системы защиты КИ путем загрузки файлов документов.	соответствует
Процесс создания индивидуального классификатора должен включать в себя: Создание категорий Обучение классификатора Проверка файлов на классификаторе Импорт и экспорт текстовых объектов в составе категории; Добавление текстовых объектов в объекты защиты.	соответствует

3.2.4 Требования к подсистеме применения политик

Требование	Выполнение требования (соответствует/не соответствует)

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.	соответствует
Подсистема применения политик должна устанавливать соответствие перехваченных и проанализированных объектов персонам, рабочим станциям и группам, полученным из службы каталогов или созданным пользователем вручную.	соответствует
Подсистема применения политик должна обеспечивать возможность объединения групп, контактов, рабочих станций, web-ресурсов в логические периметры.	соответствует
Подсистема применения политик должна предоставлять возможности для задания политик безопасности на передачу данных, копирование, хранение данных или использование буфера обмена из консоли управления.	соответствует
Подсистема применения политик должна предоставлять возможности для автоматического проставления перехваченным объектам дополнительных атрибутов (теги, уровень нарушения, вердикт) из консоли управления.	соответствует
Подсистема применения политик должна предоставлять возможность для автоматического проставления статусов сотрудникам, например, «На увольнение», «Под наблюдением» и т.д. из консоли управления.	соответствует
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.	соответствует

3.2.4.1 Требования к подсистеме интеграции со службой каталогов

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема интеграции со службой каталогов должна 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.	соответствует
Информационный обмен между Системой защиты КИ и LDAP-каталогом Active Directory должен осуществляться с использованием защищенного протокола LDAPS.	соответствует
Подсистема интеграции со службой каталогов должна предоставлять возможность настройки периода сканирования измененных элементов. При сканировании измененных элементов в	соответствует

Системе защиты КИ учитываются только изменения, произошедшие с момента последнего сканирования.	
Подсистема интеграции со службой каталогов должна предоставлять возможность настройки периода и времени сканирования службы каталогов.	соответствует
Подсистема интеграции со службой каталогов должна передавать все данные, полученные в результате импорта или синхронизации, в подсистему хранения.	соответствует
Подсистема интеграции со службой каталогов должна предоставлять возможность экспорта / импорта настроек раздела групп для дальнейшего их сохранения в качестве резервной копии или переноса на другую инсталляцию системы защиты КИ.	соответствует

3.2.4.2 Требования к подсистеме принятия решений

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема принятий решений должна обеспечивать применение политики информационной безопасности путем выполнения для объектов правил, описанных в сценариях их обработки.	соответствует
Подсистема принятий решений должна предоставлять возможности для задания правил автоматического вынесения вердикта по объекту. Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:	соответствует
формальных признаков перехваченного объекта (отправитель, получатель и т.д.), в том числе типа перехваченного объекта (всех типов данных, полученных от подсистемы перехвата трафика);	соответствует
результатов анализа перехваченных объектов от подсистемы анализа;	соответствует
форматов документов;	соответствует
статуса сотрудников («На увольнение», «Под наблюдением» и т.д.);	соответствует
логического периметра.	соответствует
Подсистема принятий решений должна обеспечивать отсутствие возможности изменения оценки событий, выносимого Системой защиты КИ автоматически на основании настроенных правил и политик.	соответствует
Подсистема принятий решений должна обеспечивать возможность информирования администратора безопасности об инцидентах путем отправки письма-уведомления об инциденте на почтовый электронный адрес.	соответствует
Подсистема принятий решений должна предоставлять возможность определять текст писем-уведомлений нарушителю, офицеру безопасности, а также любому другому получателю.	соответствует
Подсистема принятий решений должна предоставлять возможность определять текст писем-уведомлений для разных политик и вердиктов, примененных к событиям.	соответствует
Для HTTP(S)-запросов подсистема принятий решений должна определять тип сайта, на который направлен запрос, и присваивать объекту тег, соответствующий типу сайта.	соответствует

Подсистема принятий решений должна предоставлять возможности для передачи объектов в подсистему хранения.	соответствует

3.2.5 Требования к подсистеме хранения

Требование	Выполнение требования (соответствует/не соответствует)
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.	соответствует
Подсистема хранения должна осуществлять хранение данных в единой СУБД с возможностью переноса данных на медленные и быстрые диски, круговой ротацией без использования дополнительных скриптов.	соответствует
Подсистема хранения должна обеспечивать возможность устанавливать различный период хранения, как для всех объектов, так и только для объектов с нарушениями.	соответствует
Подсистема хранения должна позволять при срабатывании политики выборочно удалять из события вложения или вложения вместе с извлеченным текстом для сокращения размера архива, т.к. должна не помещать в него данные, при этом не терять информации о том, что данное событие произошло.	соответствует
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.	соответствует
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.	соответствует
Подсистема хранения должна обеспечивать отсутствие явной возможности удаления из архива Системы защиты КИ перехваченных событий, срок хранения которых меньше срока хранения, установленного в Системе Защиты КИ.	соответствует

3.2.6 Требования к консоли управления

Требование	Выполнение требования (соответствует/не соответствует)
Консоль управления 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.	соответствует

В консоли управления должна быть предусмотрена возможность проводить полный аудит действий офицера безопасности.	соответствует
В консоли управления должна быть предусмотрена возможность по разграничению прав пользователей по работе с функциями Системы защиты КИ на основании ролевой модели.	соответствует
В консоли управления должна быть предусмотрена возможность управления доступа к событиям для пользователей Системы защиты КИ.	соответствует
В консоли управления должна быть предусмотрена возможность получения детализированных отчетов в интерактивном режиме.	соответствует
В консоли управления должна быть предусмотрена возможность отображения детальной карточки события с подсветкой соответствующим цветом обнаруженных в перехваченных данных объектов защиты и терминов.	соответствует
В консоли управления должна быть предусмотрена возможность просмотра имеющихся снимков экрана рабочей станции, в том числе связанных с событием из карточки инцидента.	соответствует
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.	соответствует
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.	соответствует
В консоли управления должна быть предусмотрена возможность выгрузки карточки события и сохраненной теневой копии файлов.	соответствует
В консоли управления должна быть предусмотрена возможность управления доступа к шаблонам поиска событий и отчетам.	соответствует
В консоли управления должна быть защита от простого создания пароля и перебора пароля.	соответствует
В консоли управления должен вестись подробный журнал действий оператора параметры: поисковые запросы, старые и новые значения параметров политик при их изменении и т.д. Должна быть возможность передачи данных этого журнала во внешние системы сбора событий.	соответствует
В консоли управления должна быть предусмотрена возможность экспорта и импорта персон, групп персон и списков веб-ресурсов для переноса на другую инсталляцию системы защиты КИ.	соответствует
В консоли управления должна быть предусмотрена возможность отображения количества используемых в системе защиты КИ лицензий.	соответствует
В консоли управления должна быть предусмотрена возможность ограничить видимость информации о персонах и контактах для пользователей системы защиты КИ из различных отделов и филиалов.	соответствует
Система защиты КИ должна иметь единый интерфейс - Центр расследований, который в свою очередь должен предоставлять возможность:	соответствует

1. Объединять перехваченные события, данные о действиях сотрудников, хранении и доступе к файлам, визуальную аналитику и оповещение о грядущих рисках в информационном пространстве;	соответствует
2. Работать с необходимыми данными в одном окне и быстро переключаться между ними;	соответствует
3. Использовать единый фильтр и интерактивный интерфейс для быстрого переключения между разными срезами данных, сохранять контекст расследования и фокус на важных деталях, а также сопоставлять информацию из нескольких подсистем для быстрой интерпретации данных при принятии решений;	соответствует
4. Настроить нужное количество рабочих панелей - под каждую утилитарную задачу для обнаружения инцидентов и контроля сотрудников без дополнительных настроек фильтра;	соответствует
5. Создавать отчет о расследовании по ходу сбора обстоятельств во встроенном блокноте;	соответствует
6. Настраивать гибкие права доступа для предоставления данных смежным подразделениям.	соответствует

3.2.7 Требования к подсистеме управления клиентским программным обеспечением

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема управления клиентским программным обеспечением должна предоставлять возможность удаленной установки/обновления/удаления клиентского программного обеспечения (агента).	соответствует
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.	соответствует
Система защиты КИ должна обеспечивать возможность распространения агентов на новые АРМ за счет обнаружения в заданной группе MS Active Directory новых устройств без установленного агентского ПО.	соответствует
Система защиты КИ должна обеспечивать возможность обновления агентского ПО при использовании SMB и FTP ресурсов с целью снижения нагрузки на сетевое соединение.	соответствует
Агент Системы защиты КИ должен функционировать в среде следующих операционных систем: Microsoft Windows 10; Microsoft Windows 11; Microsoft Windows Server 2016; Microsoft Windows Server 2019;	соответствует
Microsoft Windows 10;	соответствует
Microsoft Windows 11;	соответствует
Microsoft Windows Server 2016;	соответствует

Microsoft Windows Server 2019;	соответствует
Microsoft Windows Server 2022.	соответствует
Агент Системы защиты КИ должен предоставлять возможность скрытой работы в системе и не должен обнаруживаться стандартными средствами.	соответствует
Агент Системы защиты КИ должен использовать шифрование TLS для передачи перехваченных объектов в подсистему анализа.	соответствует
Агент Системы защиты КИ должен использовать систему авторизации для предотвращения возможности подключения к подложному центральному серверу.	соответствует
Агент Системы защиты КИ должен поддерживать работоспособность в режиме SecureBoot.	соответствует

3.2.8 Требования к подсистеме анализа данных

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема анализа данных предназначена для потоковой постобработки и анализа данных, предоставляемых подсистемой анализа, подсистемой мониторинга активности. Подсистема анализа данных не должна иметь собственного графического интерфейса.	соответствует
Подсистема анализа данных должна обеспечивать возможность проводить ретроспективный анализ данных и искать в трафике идентичные документы. Должно быть реализовано два типа поиска:	соответствует
1. Поиск аналогичных документов, содержащих одинаковые термины, но созданные на базе разных шаблонов. Например, все договоры на поставку оборудования от разных контрагентов.	соответствует
2.Поиск образцов документов с одинаковой структурой, созданных в едином шаблоне, но имеющих небольшие различия в словоформах, или же полные копии. Например, все трудовые договоры сотрудников компании или все существующие черновики договоров поставки с конкретным контрагентом.	соответствует
Подсистема анализа данных должна обеспечивать возможность конвертировать аудиозапись в текст. Полученная транскрибация должна использоваться при работе с аудиозаписями в подсистеме мониторинга активности.	соответствует
Подсистема анализа данных должна детектировать непристойный контент, оружие, роскошь на рабочих станциях сотрудников. Найденный контент должен маркироваться соответствующей пиктограммой и быть доступен в разделе «Снимки экрана» в подсистеме мониторинга активности.	соответствует

3.2.9 Требования к подсистеме мониторинга прав доступа к данным

Требование	Выполнение требования (соответствует/не соответствует)

Подсистема мониторинга прав доступа к данным должна обеспечивать отслеживание изменений объектов службы каталогов, мониторинг состояния учетных записей и службы каталогов домена, а также злоупотребление правами доступа к электронной почте.	соответствует
Сервер подсистемы мониторинга прав доступа к данным должен поддерживать установку на любую из указанных операционных систем: Red Hat Enterprise Linux 7.7 и более поздние; Oracle Linux 7.9 или 8.4 и более поздние.	соответствует
Подсистема мониторинга прав доступа к данным должна обеспечивать:	
контроль изменений групп службы каталогов (создание, изменение, добавление/удаление объекта) с возможностью получить информацию о том, кем изменено и дату события;	соответствует
возможность исключить все непросмотренные события изменений групп службы каталогов или, наоборот, оставить только такие записи;	соответствует
возможность сгруппировать события изменений групп службы каталогов по следующим параметрам: группа, кем изменено, объект (пользователь), тип события;	соответствует
возможность контроля привилегированных групп, связанных с возможностью конфигурации Exchange-сервера;	соответствует
автоматический аудит прав доступа к почтовым ящикам в виде следующих отчетов:	соответствует
Отчет «Почтовые ящики с общим доступом», отображающий ящики, к которым имеют доступ другие пользователи, кроме владельца;	соответствует
Отчет «Учетные записи с доступом к ящикам других пользователей» - список пользователей и групп с доступом к почтовым ящикам других пользователей;	соответствует
автоматический аудит каталога Active Directory в виде отчетов о состоянии учетных записей и событиях службы каталогов:	соответствует
Отчет «Неактивные пользователи» - незаблокированные пользователи, неактивные 14 и более дней;	соответствует
Отчет «Неактивные компьютеры» - незаблокированные компьютеры, неактивные 14 и более дней;	соответствует
Отчет «Пользователи, не входившие в систему» - пользователи, не входившие в систему 14 и более дней;	соответствует
Отчет «Компьютеры, с которых не входили в систему» - компьютеры с недавно созданными учетными записями, откуда не выполнялся вход в систему;	соответствует
Отчет «Пользователи с постоянным паролем» - пользователи с учетными записями без указания срока смены пароля;	соответствует
Отчет «Пользователи без пароля» - пользователи с признаком Пароль необязателен;	соответствует
Отчет «Заблокированные пользователи» - автоматически заблокированные пользователи;	соответствует
Отчет «Пользователи с истекшим паролем» - пользователи с учетными записями, для которых истек срок смены пароля;	соответствует

Отчет «Неудачные попытки входа» - события неудачных попыток авторизации;	соответствует
Отчет «Изменения состава привилегированных групп» - изменения в группах с повышенным уровнем прав доступа;	соответствует
Отчет «События блокировки пользователей» - события автоматической блокировки пользователей;	соответствует
Отчет «Изменения или сброс пароля администратором» - пользователи, чей пароль был изменен администратором;	соответствует
Отчет «Подозрительная активность пользователей» - пользователи, которые начали входить в домен после длительного перерыва;	соответствует
Отчет «Изменение статуса учетных записей пользователей» - контроль создания, удаления или блокировки учетных записей пользователей;	соответствует
возможность отслеживать изменения прав доступа к важным папкам и файлам;	соответствует
возможность настройки уведомлений об изменениях в группах службы каталогов об изменениях состава привилегированных групп, в том числе и в автоматизированном режиме в выбранное время;	соответствует
возможность автоматической отправки отчетов по расписанию.	соответствует
Функционал подсистемы мониторинга прав доступа к данным должен быть в полной мере реализован в Центре расследований.	соответствует

3.2.10 Требования к подсистеме мониторинга хранилищ информации

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема должна обеспечивать сканирование файлов локальных дисков рабочих станций и серверов хранения файлов под управлением Microsoft Windows и Linux (по протоколам SMB, SSH), файлового хранилища Microsoft SharePoint Server, FTP-ресурсов (по протоколам ftp(s)), сетевых разделяемых ресурсов, с использованием следующих параметров: рабочие станции, размеры файлов и типы файлов. При передаче найденных файлов в Систему защиты КИ должна предоставляться информация о владельце и группах пользователей, имеющих к нему доступ.	соответствует
Сервер подсистемы мониторинга хранилищ информации должен поддерживать установку на любую из указанных операционных систем: Red Hat Enterprise Linux 7.7 и более поздние; Oracle Linux 7.9 или 8.4 и более поздние.	соответствует
Подсистема мониторинга хранилищ информации должна обеспечивать:	
возможность выбора из справочника масок файлов или группы масок, а также возможность экспорта в файл заданных масок для применения его в других задачах сканирования;	соответствует
возможность настраивать расписание для запуска и остановки задач сканирования с помощью следующих параметров: ежедневно, еженедельно или вручную;	соответствует
сканирование данных различных ресурсов с большой частотой;	соответствует

возможность при сканировании хоста (по протоколу SMB) самостоятельно определять существующие на нём доступные другим пользователям файловые ресурсы;	соответствует
возможность настроить интеграцию с Active Directory для добавления новых пользователей из LDAP-каталогов;	соответствует
возможность просмотра информация о найденных файлах, которую можно отфильтровать по названию, размеру, типу и дате обнаружения файла, по владельцам и правам доступа, хосту и IP адресу хоста;	соответствует
возможность проводить контентный анализ следующими способами:	соответствует
классификация конфиденциальных документов по тематике с помощью баз контентной фильтрации,	соответствует
детектирование чувствительных текстовых объектов с применением регулярных выражений,	соответствует
детектирование выгрузок из банных для защиты данных клиентов и сотрудников, номенклатуры и прайс-листов,	соответствует
детектирование заполненных бланках;	соответствует
возможность идентификации групп Active Directory для фильтрации сканированных файлов по данным группам;	соответствует
возможность копирования ссылки, содержащей полный путь к найденному файлу;	соответствует
группировка документов по смыслу с помощью технологий машинного обучения с возможностью анализа групп по характерным терминам (тэгам) и текстовому содержимому;	соответствует
возможность поиска копий файлов, идентичных указанному по содержанию с отображением всех мест расположения искомых файлов, прав доступа к ним, а также лиц, разместивших файл в хранилища или на рабочие станции;	соответствует
возможность выгрузки информации о файлах, найденных по результатам сканирования;	соответствует
возможность исключать из сканирования системные папки по предустановленному по умолчанию в систему списку с возможностью его корректировки;	соответствует
возможность отправки отчетов о результатах сканирования и правах доступа.	соответствует
Подсистема мониторинга файловых хранилищ должна обеспечивать сканирование файлов без установки программного компонента на сканируемый ресурс.	соответствует
Функционал подсистемы мониторинга файловых хранилищ должен быть в полной мере реализован в Центре расследований.	соответствует
Сервер подсистемы мониторинга хранилищ информации должен поддерживать совместную установку с подсистемой визуальной аналитики информационных потоков и подсистемой мониторинга активности пользователей, а также использовать общую ролевую модель доступа.	соответствует

3.2.11 Требования к подсистеме визуальной аналитики информационных потоков

Требование	Выполнение требования

	(соответствует/не соответствует)
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.	соответствует
Сервер подсистемы визуальной аналитики должен поддерживать установку на любую из указанных операционных систем: Red Hat Enterprise Linux 7.7 и более поздние; Oracle Linux 7.9 или 8.4 и более поздние.	соответствует
Сервер подсистемы визуальной аналитики информационных потоков должен поддерживать использование СУБД PostgreSQL.	соответствует
Для высокоскоростного исполнения аналитических запросов в режиме реального времени система должна использовать дополнительной базу данных колоночного типа. Должно обеспечиваться выполнение OLAP запросов в режиме реального времени.	соответствует
Доступ к консоли пользователя должен осуществляться через веб-интерфейс с возможностью сквозной авторизации из Системы защиты КИ.	соответствует
Подсистема визуальной аналитики информационных потоков должна обеспечивать:	соответствует
формирование динамической сводки безопасности по филиалам организации, создание единого центра статистики и управления инцидентами, в т.ч. с возможностью отображения нарушений по выбранным группам (филиалам, структурным подразделениям) или персонам, и проведения сравнительной аналитики (с последующей выгрузкой данных в отчет);	соответствует
формирование динамической сводки безопасности по всей организации или по отделам с возможностью перестраивать сводку по новым срезам данных в режиме реального времени;	соответствует
построение интерактивного графа связи для анализа связей сотрудников внутри организации и с внешними контактами с отображением интенсивности коммуникаций. Узлы и связи на графе должны быть интерактивными (с возможностью посмотреть полную детализацию по событиям и сотрудникам), а также поддерживаться фильтрация по e-mail адресам, доменам получателей, вердикту событий или категории информации с произвольной требуемой комбинацией признаков и пр. параметрам;	соответствует
отображение всех событий от всех пользователей на одном графе связей в режиме «по умолчанию» без необходимости добавления интересуемых пользователей к графу связей;	соответствует
редактирование графа связей для возможности выгрузки его в отчет и фокусировки внимания на нужных деталях. В режиме редактирования на карте коммуникаций должна быть возможность скрывать лишние элементы, перемещать узлы и объединять их в группы, например, по отделам;	соответствует

возможность периодического сохранения графа связей для возможности сравнения срезов данных между собой и отслеживания изменений с добавлением комментариев;	соответствует
возможность на графе связей визуально выделить сотрудников, которые общаются между собой интенсивнее всего для понимания реальной структуры коммуникаций в организации;	соответствует
возможность проведения экспресс-расследования с выбором конкретных событий и построением графа связи сразу по ним без перехода в другой раздел;	соответствует
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;	соответствует
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;	соответствует
отображение ресурсов с наибольшим трафиком как по количеству событий, так и по объему трафика;	соответствует
поиск событий по словам, содержащимся в теме письма;	соответствует
поиск событий по количеству вложенных файлов;	соответствует
организация доступа к деталям отображаемой информации на основании ролевой модели;	соответствует
отображение отправки сообщений самому себе на личную почту в виде кольцевых связей, фильтрацию данных по количеству получателей, использованию публичной почты;	соответствует
возможность изменения фильтра отображаемых данных без составления запросов, а выбором элемента кликом мыши на любой диаграмме;	соответствует
сохранение выявленных аномалий и комментариев офицера безопасности в поведении сотрудника в рамках досье;	соответствует
возможность открытия и просмотра сообщений мессенджеров в виде диалога для быстрой оценки ситуации, исходя из контекста и истории общения. При этом должна присутствовать возможность выбора “ID диалога” для просмотра событий конкретного диалога. В открытом диалоге должны отображаться все сообщения включая те, которые пришли с задержкой по времени и были высланы вне рамок выбранного периода;	соответствует
мониторинг состояния системы для проведения диагностики;	соответствует
возможность аккумулировать собранную из различных источников информацию по инцидентам и применять в едином расследовании для последующего принятия решения или формирования отчетов;	соответствует
возможность регулярной автоматической отправки отчетов заинтересованным лицам в заданный интервал времени: ежедневно, еженедельно или ежемесячно;	соответствует
возможность добавлять к расследованию события напрямую из списка событий,	соответствует
возможность добавлять к расследованию файл, изображение, досье сотрудника;	соответствует

возможность добавлять к расследованию текстовый комментарий.	соответствует
Функционал подсистемы визуальной аналитики информационных потоков должен быть в полной мере реализован в Центре расследований.	соответствует
Сервер визуальной аналитики информационных потоков должен поддерживать совместную установку с подсистемой предиктивной аналитики данных и использовать общую ролевую модель доступа.	соответствует

3.2.12 Требования к подсистеме мониторинга активности пользователей

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема мониторинга активности пользователей должна являться средством мониторинга, анализа, а также оценки эффективности работы сотрудников.	соответствует
Сервер подсистемы мониторинга активности пользователей должен поддерживать установку на любую из указанных операционных систем: Red Hat Enterprise Linux 7.7 и более поздние; Oracle Linux 7.9 или 8.4 и более поздние.	соответствует
Сервер подсистемы мониторинга активности пользователей должен поддерживать использование СУБД PostgreSQL.	соответствует
Для высокоскоростного исполнения аналитических запросов в режиме реального времени система должна использовать дополнительной базу данных колоночного типа. Должно обеспечиваться выполнение OLAP запросов в режиме реального времени.	соответствует
Сервер подсистемы мониторинга активности пользователей должен поддерживать совместную установку с подсистемой визуальной аналитики данных и использовать общую ролевую модель доступа.	соответствует
Подсистема мониторинга активности пользователей должна предоставлять возможность установить в систему собственный сертификат для защиты https-подключений.	соответствует
Подсистема мониторинга активности пользователей должна обеспечивать:	
перехват и хранение информации снимков экранов с настраиваемой периодичностью;	соответствует
перехват нажатий клавиш с клавиатуры на рабочем месте, отображение вводимого текста;	соответствует
возможность категоризации посещенных сайтов, запускаемых приложений, на тематические группы, используя локальный классификатор;	соответствует
возможность создания снимков экрана по заданному расписанию для приложений и web сайтов;	соответствует
возможность записывать и прослушивать аудиозаписи с микрофона и динамика рабочей станции сотрудника по триггеру – переходу на веб-сайт (сервис онлайн-конференций, конференцсвязи или любой другой), а также с момента авторизации на рабочей станции до выхода из сессии пользователя. При прослушивании аудиозаписей	соответствует

должна обеспечиваться возможность размечать на временной шкале отрезки с важной информацией;	
получение информации о деятельности сотрудника в реальном времени с экранов/микрофонов рабочей станции;	соответствует
возможность записывать видео в режиме реального времени экрана рабочей станции сотрудника;	соответствует
отображение информации о действиях сотрудников в реальном времени с отображением последних снимков экрана;	соответствует
получение информации о запущенных процессах в реальном времени с возможностью блокировки рабочей станции;	соответствует
возможность просмотра интерактивного таймлайна с возможностью масштабирования, где в единой временной ленте будут представлены все события входов/выходов, использования приложений, веб-сайтов, вводимый текст, снимки экрана, файловые операции, аудиозаписи, а также рабочее расписание и разметка по типам активности;	соответствует
возможность анализа и контроля подключенных устройств с указанием идентификатора устройства, события подключения/использования/записи с выгрузкой в отчет;	соответствует
выгрузки всех данных из виджетов экрана и списка событий в один Excel-файл с сохранением настроек фильтров, при помощи которых были отобраны данные;	соответствует
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). Эти данные должны дополняться расписанием в календаре пользователя в MS Outlook и отображаться в отчете;	соответствует
возможность актуализации рабочего расписания данными из кадровой системы 1С. Рабочее расписание должно автоматически синхронизироваться и учитывать данные о больничных, отпусках и командировках;	соответствует
сравнение данных за два различных периода по следующим срезам данных: Тип активности, Топ приложений, Топ веб-сайтов, Активность по часам, Время работы с возможностью сохранить результаты сравнения в виде изображения;	соответствует
получение детальной информации о встречах, запланированных в календаре MS Outlook (тема встречи, место, список участников, продолжительность, детали);	соответствует
возможность создания рабочего расписания, указав периоды рабочего и нерабочего времени для конкретного сотрудника, группы сотрудников или всех сотрудников организации;	соответствует
учитывать график работы сотрудников с учетом праздничных и нерабочих дней, дни во время отпуска, время предполагаемого прихода и ухода. Учитывать возможность установки сокращенного рабочего дня в рабочей неделе. Учитывать производственный календарь.	соответствует
должна обеспечиваться возможность интеграции с любым СКУД, поддерживающим выгрузку данных через CSV-файл;	соответствует

возможность проведения учета лицензий используемого ПО, путем внесения информации о количестве лицензий и часов использования из статистики с последующей выгрузкой в отчет со статистикой использования ПО;	соответствует
возможность отслеживать события отправки документов на печать для формирования статистики по сотрудникам и принтерам;	соответствует
возможность указать число лицензий для выбранных категорий ПО в справочнике для выгрузки детализированного отчета по статистике использования ПО;	соответствует
мониторинг и отображение отчетов по активности пользователя с папками и файловыми операциями (создание, копирование, редактирование, удаление, перемещение и тд.) на рабочем месте с возможностью выгрузить отчет в формате XLS;	соответствует
формирование карточки события, в которую помещается информация: фото сотрудника; имя и фамилия сотрудника; тип события; рабочая станция сотрудника, на которой произошло событие; дата и время создания события; тип активности; приложение, которое использовалось; время активной работы с приложением; общее время работы; правило маркировки. отображение сводной статистики по данным в виджетах: «Лента активности»; «Топ приложений»; «Активность по дням»; «Время работы»; «Тип активности»; «Топ сайтов»; «Топ приложений».	соответствует
формирование интерактивного досье на сотрудника организации с отображением детализации по событиям;	соответствует
отображение временной шкалы, на которой отмечена рабочая и нерабочая активность сотрудника, а также отметки о сделанных снимках экрана, с возможностью перемещения по данной шкале для просмотра соответствующих снимков экрана;	соответствует
автоматически отправлять уведомления по фактам нерабочей активности сотрудников в приложениях и веб-сайтах, а также по определенным веб-сайтам, заданным заранее за предыдущие сутки;	соответствует
возможность регулярной автоматической отправки отчетов заинтересованным лицам в заданный интервал времени: ежедневно, еженедельно или ежемесячно;	соответствует
отображение снимков экрана в виде слайд-шоу. Возможность группировки снимков по активным сессиям, а также в режиме наложения на шкалу времени событий работы в приложениях и посещения веб-сайтов;	соответствует

возможность проводить экспресс-расследование с дополнением конкретного события скриншотами и таймлайном действий сотрудника без перехода в другой раздел;	соответствует
табличное представление следующих данных:	соответствует
общее время, когда компьютер сотрудника работал;	соответствует
активное время, когда сотрудник работал и выполнял какие-то операции на компьютере;	соответствует
неактивное время, когда сотрудник бездействовал;	соответствует
первая активность за сутки, когда сотрудник в выбранную дату приступил к работе;	соответствует
последняя активность за сутки, когда сотрудник в выбранную дату закончил работать.	соответствует
возможность экспорта всех выбранных снимков экрана;	соответствует
возможность создания и присвоения произвольных тэгов событиям и снимкам экрана с последующей возможностью фильтрации событий по тэгам;	соответствует
возможность изменения фильтра отображаемых данных без составления запросов, а выбором элемента кликом мыши на любой диаграмме;	соответствует
возможность переключения между подсистемой мониторинга активности пользователей и подсистемой визуализации информационных потоков при помощи единой консоли;	соответствует
возможность использования единого фильтра для мгновенной фильтрации событий и отображения необходимого среза статистики в режиме реального времени;	соответствует
возможность отключить из анализа события, которые были созданы на ПК вне деятельности пользователя (системные процессы / события на заблокированном ПК);	соответствует
возможность использования масок при добавлении ресурсов в справочники системы (например,*.example.ru).	соответствует
Функционал подсистемы мониторинга активности пользователей должен быть в полной мере реализован в Центре расследований.	соответствует

3.2.13 Требования к подсистеме предиктивной аналитики

Требование	Выполнение требования (соответствует/не соответствует)
Подсистема предиктивной аналитики данных должна являться средством выявления аномалий в поведении сотрудников и уведомлений о группах риска.	соответствует
Сервер подсистемы предиктивной аналитики данных должен поддерживать установку на любую из указанных операционных систем: Red Hat Enterprise Linux 7.7 и более поздние; Oracle Linux 7.9 или 8.4 и более поздние.	соответствует
Подсистема предиктивной аналитики данных должна обеспечивать:	
автоматический анализ и выявление аномалий в поведении сотрудников на любых контролируемых каналах (например, почта,	соответствует

браузеры, мессенджеры, облачные хранилища, внешние накопители, принтеры);	
автоматический анализ передаваемой по контролируем каналам информации и автоматическое выявление аномалий по результатам этого анализа; в том числе:	соответствует
лингвистический анализ (например, использование нецензурной лексики, негативные отзывы о работодателе, обсуждение увольнения);	соответствует
пересылка документов определенной категории;	соответствует
автоматическое выявление аномалий в действиях контролируемых персон по нескольким параметрам в совокупности;	соответствует
использование выявленных аномалий для определения принадлежности персоны к группе риска: Подготовка к увольнению, Аномальный вывод информации, Отклонение от бизнес-процессов, Снижение производительности, Нетипичные внешние коммуникации, Нелояльные сотрудники, Интерес к СВО, Политические взгляды;	соответствует
возможность посмотреть краткий комментарий, почему именно сотрудник попал в группу риска. Детализация рейтинга тезисно должна указывать на выявленные паттерны поведения и конкретные причины – регулярные или участившиеся события, а также детализация соответствующих событий из Системы защиты КИ;	соответствует
просмотр и сравнение в рамках одного экрана автоматически выявленных аномалий в поведении одного или нескольких сотрудников как из одного, так и из разных отделов;	соответствует
отображение групп риска в виде кликабельных карточек с помощью которых должна быть возможность просмотра количества сотрудников, находящихся в группе риска, а также сколько сотрудников было добавлено/исключено из группы за выбранный период;	соответствует
получение и анализ событий подключения\блокировки съемных устройств;	соответствует
возможность «перейти» для получения деталей по автоматически выявленным аномалиям из подсистемы предиктивной аналитики данных в DLP-систему;	соответствует
отправку уведомлений об ухудшении рейтинга сотрудников;	соответствует
возможность выгрузки отчетов с данными по группе риска, рейтингу и динамики аномалий;	соответствует
возможность просмотра карты паттернов на виджете, который отображает выявленные паттерны на основании действий персоны в заданной последовательности.	соответствует
Функционал подсистемы предиктивной аналитики должен быть в полной мере реализован в Центре расследований.	соответствует
Сервер подсистемы предиктивной аналитики данных должен поддерживать совместную установку с подсистемой мониторинга	соответствует

активности пользователей и использовать общую ролевую модель доступа.	

3.3 Перспективы развития и модернизации Системы защиты КИ

Требование	Выполнение требования (соответствует/не соответствует)
Система защиты КИ должна обеспечивать возможность модернизации путем замены технического и/или программного обеспечения.	соответствует
Система защиты КИ должна допускать расширение функциональных возможностей за счет дополнительных компонентов, требования к которым описаны ниже. Описанные компоненты не должны требовать дополнительной разработки со стороны производителя программного обеспечения, используемого при построении Системы защиты КИ.	соответствует
Система защиты КИ должна обеспечивать возможность контроля файловых операций и перехвата файлов, который пользователь получает или отправляет другим адресатам при использовании desktop приложения сервиса: WinSCP 7Zip WinRar	соответствует
В момент перехвата теневой копии файла должен создаваться скриншот экрана.	соответствует
Система защиты КИ должна обеспечивать возможность интеграции с внешними системами за счёт использования различных API (программных интерфейсов приложения), функционал которых описан ниже.	соответствует
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.	соответствует
API, применяемого для автоматической загрузки «Эталонных выгрузок баз данных» и «базы цифровых отпечатков» из сторонних систем.	соответствует
API, применяемого для отправки содержимого и метаданных событий из Системы защиты КИ в различные сторонние системы.	соответствует
Система защиты КИ должна предоставлять возможность интеграции с системами класса SIEM (MaxPatrol, QRadar, Wazuh и др.) для отправки событий из Системы защиты КИ в системы класса SIEM.	соответствует

4. Требования к документации

№	Документ	Требования к документу
1	Отчет об обследовании текущей инфраструктуры	Электронный документ на русском языке; Формат - docx
2	Техническое задание на внедрение	Электронный документ на русском языке; Формат – docx; Документ должен быть согласован с заказчиком по электронной почте.
3	Концепция настройки политик	Электронный документ на русском языке; Формат – docx; Документ должен быть согласован с заказчиком по электронной почте.
4	Паспорт Системы защиты КИ	Электронный документ на русском языке; Формат – docx; Документ должен быть согласован с заказчиком по электронной почте.
5	Программа и методика испытаний	Электронный документ на русском языке; Формат – docx; Документ должен быть согласован с заказчиком по электронной почте.
6	Руководство администратора	Электронный документ на русском языке; Формат – docx; Документ должен быть согласован с заказчиком по электронной почте.

В процессе подготовки каждого отдельного результата из таблицы выше (далее – Результаты) Исполнитель должен взаимодействовать с Заказчиком.

Обязанность по подготовке Результатов считается исполненной после учета всех комментариев Заказчика и направления Заказчиком Исполнителю уведомления о принятии Результата.

Таблица соответствия требованиям Системы защиты КИ и инструкция по ее заполнению приведена в Приложении к настоящему Техническому заданию.

5. Требования к исполнителю

Исполнитель должен иметь партнерский статус с производителем программного обеспечения Системы защиты КИ (для подтверждения соответствия данному требованию Исполнитель должен предоставить копии соответствующих сертификатов и авторизационное письмо), либо являться производителем программного обеспечения Системы защиты КИ.

Исполнитель должен иметь опыт реализации проектов по поставке программного обеспечения и внедрения систем информационной безопасности не менее 3 лет (подтверждается копией договоров, накладных и актов выполненных работ).

Исполнитель должен обладать лицензией ФСТЭК России на услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации (подтверждается копией соответствующей лицензии).

Исполнитель должен иметь следующие сертификаты соответствия:

сертификат соответствия системы менеджмента качества организации требованиям международного стандарта ISO 9001-2011 (ISO 9001:2008);

сертификат соответствия системы менеджмента информационной безопасности организации (ISO/IEC 27001:2005) требованиям ГОСТ Р ИСО/МЭК 27001-2013;

сертификат соответствия системы менеджмента услуг в области информационных технологий (IT сервис) организации требованиям ГОСТ Р ИСО/МЭК 20000-1-2013 (ISO/IEC 20000-1:2011);

Исполнитель должен иметь в штате организации подразделение, осуществляющее сервисные функции с численностью персонала не менее 5 человек (подтверждается копией положения и выпиской из штатного расписания). Исполнитель должен иметь информационную систему приема и обработки заявок по технической поддержке, действующую в режиме 24х7х365 (подтверждается информационным письмом в свободной форме, оформленным на бланке компании-участника, за подписью уполномоченного представителя).

Исполнитель должен иметь уставной капитал организации в размере не менее 500 000 рублей.