№ 18-02-16-11
2022yil «20» iyun

УТВЕРЖДАЮ
Первый заместитель
АО "Узавтосаноат"
Рафиков А.В.

"____"_____ 2022г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ЗАКУПКУ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРЕДНАЗНАЧЕННОЕ ДЛЯ ЗАЩИТЫ КОМПАНИИ ОТ УТЕЧКИ ИНФОРМАЦИИ DLP

г. Ташкент, 2022г.

Требования на внедрение системы

Работы по внедрению должны быть выполнены в течении 15 дней.

ОПИСАНИЕ ЭТАПОВ:

Этап 1. Проектирование.

Этап 2. Установка. Общая настройка системы управления.

Этап 3. Настройка модулей

Этап 4. Опытная эксплуатация, проверка работоспособности.

Этап 5. Обучение

ЭТАП 1. ПРОЕКТИРОВАНИЕ:

ОБСЛЕДОВАНИЕ:

Сбор информации о необходимых каналах мониторинга (SMTP, HTTP, HTTPS, FTP и т.д.) на периметре компании;

Определение операционных систем конечных точек, на которых будет установлен агент мониторинга (рабочие станции сотрудников);

Определение перечня систем, на которых будет производиться поиск конфиденциальных данных (рабочие станции, файловые сервера общего доступа)

Определение средств/методов распространения агентов на рабочие станции и обновления конфигураций

Открытие сетевых доступов, необходимых для работы комплекса DLP.

РАЗРАБОТКА ТЕХНИЧЕСКИХ И СИСТЕМНЫХ РЕШЕНИЙ:

Разработка архитектуры DLP (состав, размещение компонентов) с учетом требований по отказоустойчивости и обеспечению надежности;

Разработка детального перечня каналов мониторинга на

периметре компании;

Обзор перечня источников данных, с которых буду сняты отпечатки конфиденциальной информации (предоставляется заказчиком);

Согласования перечня конечных рабочих станций пользователей и серверов, на которых будет развернут агент DLP;

Разработка правил и политик срабатывания по стандартным шаблонам системы.

РАЗРАБОТКА ДОКУМЕНТАЦИИ ВНЕДРЕНИЯ:

Разработка схемы установки со связкой сопутствующими компонентами.

ЭТАП 2. УСТАНОВКА. ОБЩАЯ НАСТРОЙКА СИСТЕМЫ:

Установка виртуальных образов системы;

Настройка интерфейсов управления комплексом DLP

Первоначальная настройка, включая TCP/IP настройки.

Установка дополнительных компонентов при необходимости;

Подключение и связка с менеджментом;

Установка актуальной версии и последних обновлений всех компонентов системы DLP

Смена паролей по умолчанию;

Настройка интеграции со службой каталогов.

Заведение пользователей и настройка аутентификации через корпоративный LDAP сервер;

Разграничение прав доступа к системе (администратор, офицер безопасности, другие роли), возможность создания пользовательских ролей.

Протоколирование действий участников системы (администраторов, офицеров безопасности и т.д.)

Настройка синхронизации времени с корпоративными NTP

серверами;

Настройка интеграции с почтовым сервером для отправки уведомлений.

Настройка системы оповещения о нештатных ситуациях.

Снятие слепков с конфиденциальной информации, которая будет являться критерием срабатывания политик (слепки с баз данных, файлов), не более 15 слепков.

Базовая настройка системы.

Создание политик не более 10 для определения конфиденциальных данных.

ЭТАП 3. НАСТРОЙКА МОДУЛЕЙ

Создание и предоставление дистрибутива для групповой установки агентов на рабочие станции пользователей.

Установка агентов на рабочих станциях используя групповые политики либо Microsoft SMS/SCCM (не менее 10 рабочих мест)

Установка агентов мониторинга (не менее 10 рабочих станций) с использованием групповой политики

Защита агента безопасности от удаления пользователем.

Настройка политик, по умолчанию до 10.

Настройка периодического сканирования нескольких ресурсов общего доступа на наличие конфиденциальных данных (не более 2 – файловый ресурс)

Настройка поиска конфиденциальных данных в базе данных при необходимости;

Настройка политик (не менее 15) реагирования на обнаруженный контент;

Настройка политик системы на периметре компании по контролю мониторингу/блокировке контента каналов SMTP (интеграция с почтовым сервером), настройка правил для данного режима работы.

Проверка состояния каналов – отсутствие перегрузки, ошибок.

Модуль подключается в два этапа: тестовый и продакшен. На тестовом этапе запускаем тестовые сообщения для определения работоспособности.

Проверка регистрации соответствующих инцидентов.

Настройка политик (не менее 10) реагирования на обнаруженный контент

ЭТАП 4. ОПЫТНАЯ ЭКСПЛУАТАЦИЯ, ПРОВЕРКА РАБОТОСПОСОБНОСТИ.

Критерии проверки работоспособности системы:

Возможность блокировки отправки конфиденциальной информации по основным каналам коммуникаций (веб-браузер, веб-приложения, почтовая система) и при работе на конечном компьютере.

Регистрация инцидентов безопасности по сетевым каналам и на конечном компьютере в одной системе с информации о нарушителях из службы каталогов.

Единая политика защиты от утечек данных, применяемая и к сетевым каналам, и к конечным компьютерам, настраиваемая однократно в одном интерфейсе.

Обнаружение признаков конфиденциальных документов в файловых хранилищах, при работе с веб-приложениями, почтовой системой, на конечном компьютере и при копировании на съемные носители.

Контроль следующих операций на конечном компьютере: копирование и вставка из буфера обмена, копирование файла по LAN, локальная печать.

Обнаружение номеров пластиковых карт при отправке по основным каналам бизнес-коммуникаций и при работе на конечном компьютере.

Автономная работа агента безопасности на конечном компьютере с сохранением всех аналитических функций (включая защиту персональных данных) при потере связности с сервером

управления.

Опциональное шифрование конфиденциальных файлов при копировании на съемные носители.

Защита агента безопасности от удаления пользователем.

Импорт пользователей из имеющихся служб каталогов.

Ролевое разделение пользователей системы с независимым доступом к функциям системного администрирования, настройке политик и управлению инцидентами; возможность ограничения доступа администраторов к инцидентам и копиям сообщений.

Возможность входа в интерфейс администрирования с учетной записью из служб каталогов.

Построение отчетности по инцидентам с возможность экспорта во внешние системы.

ЭТАП 5. ОБУЧЕНИЕ

Провезти обучение администрированию и настройки системы DLP ,1 штатного сотрудника (администратора системы)

Требование к закупу прилагается в приложении1

Утверждение

Первый заместитель председателя правления	2022-06-20 10:16	**А. В. Рафиқов**

Согласование

Инспектор по делопроизводству 02	2022-06-20 09:51	**А. Ш. Анваржонов**
Начальник управления	2022-06-20 09:36	**А. М. Рустамов**

Главный специалист **В. О. Серикова**

2022-06-17 17:39

Согласование внутри подразделение

Начальник управления **Г. Р. Хусаинов**

2022-06-17 17:38

Ответственный

Главный специалист по информационной безопасности **С. Р. Тухтамишев**

2022-06-17 17:37

Техническое задание на закупку специализированного программного обеспечения, предназначенное для защиты компании от утечек информации DLP

Система DLP	1) **Система DLP должна поддерживать не менее 100 пользователей.** 2) **Единая консоль управления, которая может использоваться для различных направлений защиты: DLP, WEB, EMAIL.** Унифицированная платформа, которая может сочетать контроль не только DLP, но также WEB и EMAIL, которые могут понадобиться в будущем. WEB, EMAIL - это отдельные продукты, но управление идет с одной консоли, так же, как и DLP. 3) **Консоль управления DLP должна работать на базе Windows Server-а (не менее 2019) и использовать MS SQL (не менее 2019 Standard или Enterprise) базу данных для настроек и для инцидентов.** 4) **Поддерживаемые ОС для DLP на уровне клиентского компьютера: Windows 7, 8, 8. 1, 10, Server 2012 R 2, Server 2016, Server 2019, Mac OS X 10.11.6-11.1.** 5) **Возможность использовать агент DLP на VDI (Virtual Desktop Infrastructure): Citrix Virtual Apps 1912 LTSR, Citrix XenApp 7.15 LTSR CU 4, VMWare Horiz on 7.9.** 6) **Система должна иметь единый инсталлятор агента для ПК, как DLP, так и для CASB решения, который выполняет основную функцию по предотвращению конфиденциальных данных на различные каналы связи, в том числе и облачные приложения – G Suite.** 7) **Система DLP должна иметь отдельный модуль для интеграции по ICAP с прокси сервером, и дополнительно, иметь интеграцию с почтовым сервером Exchange, как MTA сервер, которые общаются через SMTP протокол. Также, этот модуль должен принимать через SPAN трафик от заданных заказчиком сетевых устройств.** 8) **Обязательно наличие функционала/модуля для поиска конфиденциальной информации по сети и в базах данных.**

	9) **Система DLP должна сохранять теневые копии данных по которым были инциденты. Эта функция должна выключаться для некоторых правил.** 10) **Функционал оптического распознавания текста (OCR) в реальном времени для переданных и сохраненных конфиденциальных данных должен быть встроенным в решение DLP, без дополнительных лицензий.** 11) **Работа OCR должна быть на сетевом уровне и на уровне CASB для облачных приложений G Suite.** 12) **Система OCR должна иметь полную поддержку узбекского и русского языка.** Учитывая, что данные передаются по сети и сохраняется в виде сканированных документов, а также снимков экрана. Данные могут содержать любую конфиденциальную информацию и коммерческую тайну, такие данные необходимо выявлять в реальном времени, и реагировать в соответствии с политикой DLP. 13) **Поддержка типов классификаторов, данных:** По ключевым словам, и словарям, регулярным выражениям, по свойству файла, с помощью машинного обучения, готовым скриптам и по цифровым отпечаткам. 14) **Регистрация конфиденциальных документов с помощью цифровых отпечатков.** Специализированные средства DLP для защиты конфиденциальных документов должны иметь возможность регистрации документов в необратимом виде (метод цифровых отпечатков), с целью выявить следующую передачу даже измененных фрагментов текста путем измерения степени сходства текстов. При этом не допускается внесение каких-либо тегов, меток, метаданных и других маркеров в файлы. 15) **Выявление нестандартного шифрования.** 16) **Выявление конфиденциальной информации на агентах.** Эта функция должна быть встроена в агент для поиска конфиденциальной информации на установленных агентах компании. 17) **Возможность блокировки серий незначительной утечки.** Для обхода механизма DLP злоумышленник может использовать длинную серию из коротких утечек, отправленных в течение определенного времени. Их необходимо выявлять и блокировать. 18) **Шаблоны для защиты персональных данных, включающих словари имен и скрипты для сложных**

	алфавитно-цифровых объектов. Система должна иметь не менее 1500 готовых шаблонов для выявления конфиденциальных данных, в том числе и отдельные шаблоны по выявлению персональных данных. 19) **Система должна уметь осуществлять анализ HTTPS трафика.** 20) **Автономная работа агента для рабочих станций, с сохранением отпечатков документов и таблиц.** Агент DLP, работающий на рабочей станции, должен быть готовым к обрывам связи с сервером управления, с сохранением функций защиты зарегистрированных данных. 21) **Защита от кражи файлов с хэшам и паролей.** 22) **Решение DLP должно иметь бесплатный модуль по расследованию инцидентов для определения рейтинга риска инцидентов.** 23) **Защита от попадания конфиденциальной информации на мобильных устройствах сотрудников через почту по протоколу ActiveSync** т.е. система должна обеспечить ограничение на ведение конфиденциальной переписки с мобильных устройств, путем фильтрации сообщений, загружаемых на устройство при синхронизации. 24) **Система должна иметь библиотеку готовых классификаторов конфиденциальных данных - более 1500 шаблонов от вендора.** 25) **Поддержка возможности расширения защиты решениями классификации данных** Система DLP должна иметь возможность обнаружения классификации и интегрироваться с надежными поставщиками IRM, такими как: Microsoft и BJ (Boldon James). 26) **Географический контроль утечек данных с учетом Интернет-категорий** Система контроля утечек, данных по веб-каналам должна в реальном времени учитывать регион (страну), где находится веб-сервер, а также категорию сайта (например, банковские сайты, бесплатная веб-почта, социальные сети, и т.д.). Эта информация должна использоваться для принятия решений о блокировании операции, например, запретить отправку персональных данных на серверы, расположенные в других странах, запретить публикацию документов в социальных сетях и т.д. Эта же информация нужна и для отчетности: каждое событие, которое зарегистрировано как

	предполагаемый инцидент, должен содержать информацию о регионе (стране) и категории Интернет-сайта. 27) **Поддержка агентом для рабочих станций работы в среде Apple Mac OS** Система должна предотвращать утечки данных непосредственно на компьютерах пользователей под управлением Apple Mac OS, включая полный контроль содержания файлов, копируемых на отчуждаемые носители. Содержание должно контролироваться с применением всех действующих политик, включая зарегистрированные в системе файлы и таблицы базы данных. Временная потеря сетевой связи между рабочей станцией и сервером управления никак не должна ограничивать функции безопасности на рабочей станции. 28) **Прямая и обратная совместимость между различными версиями программного обеспечения сервера управления и агента для рабочих станций** Обновления программного кода агентов на рабочих станциях на более новую версию не должно требовать обновить сервера управления на ту же версию. И наоборот, обновление программного кода сервера управления на новую версию не должно требовать обновить агентов на рабочих станциях на ту же версию. В обоих случаях требуется полное сохранение всех функций безопасности на рабочих станциях, действовавших до обновления программного кода. 29) **Система DLP должна иметь возможность подключения к CASB того же производителя для контроля облачных приложений (office365, g suite).** 30) **Включение в техническую поддержку услуги по созданию классификаторов данных.** 31) **Обучение сотрудников ИБ администрированию и настройки системы DLP** Профессиональные услуги производителя ПО экономят ресурсы заказчика на изготовление сложных классификаторов данных. В случае, когда для конфиденциальных данных сложно создать классификатор вручную, необходимо иметь возможность обратиться с техническим заданием к производителю и получить доработки продукта в рамках действующего контракта технической поддержки. **Возможность загрузки обновлений и исправлений программного обеспечения.**