**Техническая Спецификация**

**Общее положения**

Программно-аппаратный комплекс DLP (Data Loss Prevention) для модуля офисного контроля, предназначенного для мониторинга действий и контроля сотрудников.

Информационная сеть Банка включают в себя 500 рабочих станций пользователей и территориально распределена по разным офисам на всей территории Кыргызской Республике.

**Цель DLP – системы модуля офисного контроля**

Для каких целей нужно внедрение новой DLP системы модуля офисного контроля:

* расследования инцидентов ИБ;
* сбора доказательной базы;
* контроля эффективности персонала;
* получения расширенных отчетов по продуктивности персонала.

**Задачи, решаемы DLP – системой модуль офисного контроля**

DLP – система модуль офисного контроля должна отслеживать:

* Мониторинг корпоративной электронной почты (личных при необходимости);
* Посещение сайтов;
* Использование приложений и веб‑ресурсов;
* Запросы в поисковиках;
* Вводимый текст;
* Действия с файлами и папками;
* Подключение внешних устройств;
* Рабочая и нерабочая активность;
* Звук онлайн‑конференций;
* Звук с микрофона и видео с экрана ПК в реальном времени;
* Снимки экрана — регулярно и при смене активного окна (либо другие настройки);
* Вход и выход из помещения (если есть интеграция со СКУД системой).

**Общие требование к DLP – системе модуля офисного контроля.**

* Система должна быть основана на клиент серверной архитектуре.
* Все компоненты системы должны быть от единого правообладателя для обеспечения совместимости и надежности работы.
* В систему должен входить следующий состав компонентов:
* сервер администрирования - работает как сервис на выделенном сервере обеспечивает связь между базой данных и другими компонентами системы, позволяет удаленно управлять клиентами;
* консоль управления - используется для управления сервером удаленного администрирования, настройки и отображения данных системы;
* консоль отчетов - используется для отображения отчетов, о клиент/агент - устанавливается на рабочих станциях;
* база данных - используется для хранения полученных данных и настроек.
* Интеграция с MS Active Directory;
* Регулируемая централизованная консоль администрирования;
* Изменяемые права доступа к результатам и настройкам продукта, управление правами доступа к администрированию;
* Скрытый режим работы агента на конечной станции, в том числе, для процессов и папок, должен скрываться даже для локального и доменного администратора (если такая имеется);
* Система защиты от перехвата. Должна быть активна для пользователей, локального и доменного администратора;
* Отсутствие возможности остановить процессы, в случае более высоких прав продукт перезапустит остановленные процессы или использует другой способ сохранения данных процессов запущенными;
* Отсутствие возможности удалить продукт без прямого разрешения;
* Отсутствие возможности изменить настройки с конечной точки;
* Наличие способа защиты клиента в безопасном режиме;
* Функциональность должна сохраняться в автономном режиме, при подключении к другой локальной сети или к интернету;
* Возможность экспорта отчетов;
* Возможность отправлять отчеты и логи в систему SIEM;
* Хранение отчетов об анализируемых данных и поиск по ним;
* Управление долгосрочным хранением;
* Решение должно поддерживать или иметь возможность предоставлять резервные копии своих собственных компонентов, особенно записей и конфигураций;
* Автоматическая генерация отчетов по электронной почте в случае инцидентов;
* Возможность изменения уровней чувствительности и спецификаций инцидентов;
* Проведение расследований по факту выявления утечек конфиденциальной информации за пределы Банка.
* Автоматическая генерация отчетов по электронной почте с возможностью полной настройки (объем информации, схема отслеживаемых пользователей, частота отправки, получатели).
* Решение должно поддерживать инспекцию SSL на защищаемых устройствах с использованием собственных SSL сертификатов для предоставления базового уровня безопасности и шифрования данных, а также поддерживать возможность импорта используемых заказчиком SSL сертификатов.

**Требования к функциям системе контроля пользователей и приложений:**

* мониторинг корпоративной почтовой системы;
* мониторинг корпоративного мессенджера;
* мониторинг действий сотрудников на рабочих станциях;
* мониторинг корпоративных файловых ресурсов;
* сбор и накопление информации о сотрудниках;
* профилирование активности сотрудников на основе встроенных инструментов анализа;
* после истечении сроков лицензии функции системы оставались активны.

**Требования к серверному оборудованию**

* Процессоры с многими ядрами и высокой тактовой частотой (производительность чтобы был избыточен)
* Объем оперативной памяти (RAM): 64 GB и более (производительность чтобы был избыточен)
* DLP системы могут генерировать большие объемы аудиторских и событийных данных, поэтому сервер должен быть оснащен достаточным объемом хранилища для сохранения данных от 3 месяца до 1 года и были оснащены надёжными накопителями, такие как SSD или NVMe SSD, для обеспечения быстрого доступа к данным дополнительно оснащен большими объемами HDD для хранения архивных данных от 1 года до 3 лет.
* Сервер должен иметь достаточное количество сетевых портов и поддерживать высокие скорости передачи данных для обеспечения эффективного мониторинга и защиты сетевого трафика.
* Серверное оборудование должно поддерживать возможность расширения процессоров, оперативной памяти и хранилища данных.

**Требования к аппаратному и программному обеспечению**

Системные требования для использования программного обеспечения не должны превышать следующие характеристики аппаратного обеспечения: Системные требования к оборудованию описаны с учетом не более 500 пользователей/агентов.

***Сервер DLP-системы:***

-16-ядерный процессор с частотой не менее 2,4 Ghz(при необходимости больше);

-32 Gb ОЗУ (при необходимости больше);

-300 Gb свободного дискового пространства;

***Сервер СУБД:***

-16-ядерный процессор с частотой не менее 2,4 Ghz(при необходимости больше);

-16 Gb ОЗУ(при необходимости больше);

4 Tb свободного дискового пространства(при необходимости больше);

***Консоль управления:***

-4-ядерный процессор с частотой не менее 2,4 Ghz;

-8 Gb ОЗУ;

-5 Gb свободного дискового пространства;

Поддерживаемые операционные системы: о Microsoft Windows 10(х86-64), более новые версии операционной системы Windows.

***Консоль отчетов:***

-4-ядерный процессор с частотой не менее 2,4 Ghz;

-8 Gb ОЗУ;

-5 Gb свободного дискового пространства;

Поддерживаемые операционные системы: о Microsoft Windows 10(х86-64), более новые версии операционной системы Windows.

***Веб-консоль управления системой DLP (если такая имеется):***

-4-ядерный процессор с частотой не менее 2,4 Ghz;

-8 Gb ОЗУ;

-20 Gb свободного дискового пространства;

***Веб консоль должна быть совместима со следующими версиями веб-браузеров:***

Chrome 101 и новее;

Firefox 101 и новее;

Edge 101 и новее;

Safari 16 и новее.

***Рабочие станции:***

-2-ядерный процессор с частотой не менее 2,4 Ghz;

-4 Гб ОЗУ;

2 Гб свободного дискового пространства; -

Поддержка Windows 7, 8.1, 10, 11 полной функциональностью;…

**Требования хранения событий к программно-аппаратному комплексу DLP системы модуля офисного контроля:**

Хранение событий в программно-аппаратном комплексе DLP-системе играет ключевую роль в обеспечении безопасности и аудита информации и данные требование должны удовлетворять следующим параметрам:

* централизованное хранение истории инцидентов;
* поддержка хранения данных на клиентских станциях при отсутствии связи с сервером управления;
* использование СУБД для хранения данных;
* система хранения событий должна обеспечивать быстрый доступ к данным сроков события от 1 месяца до 3 месяцев;
* события должны храниться на долгосрочной основе от 1 года –до 3 лет;
* удобная архиваций старых или малозначимые события могут быть для экономии ресурсов хранилища и оптимизации производительности системы;
* архивированные данные должны быть легко доступны для анализа при необходимости;
* хранилище событий должно быть масштабируемым, чтобы обеспечить возможность хранения больших объемов данных, которые могут возникнуть в результате длительного мониторинга и анализа событий.

**Требования к эксплуатационной документации**

Эксплуатационная документация для программных продуктов средств офисного контроля сотрудников, включая средства управления, должна включать документы:

руководство пользователя (администратора);

руководство администратора средств удаленного администрирования.

Документация, поставляемая с программными продуктами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства офисного контроля сотрудников.

**Требования к технической поддержке**

Техническая поддержка программного обеспечения средства офисного контроля сотрудников должна:

* предоставляться на русском языке сертифицированными специалистами производителя круглосуточно без праздников и выходных (24/7) по электронной почте и через интернет, а также по телефону;

веб-сайт ПО должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, пополняемую базу знаний и русскоязычный форум.