

Обґрунтування технічних та якісних характеристик предмета закупівлі, його очікуваної вартості

Вимоги щодо технічних та якісних характеристик встановлено відповідно до потреби замовника в обладнанні, що повинне забезпечити захист конфіденційних даних та запобігання їх витоку в Апеляційній палаті Вищого антикорупційного суду.

Програмне забезпечення повинне відповідати наступним технічним вимогам:

- Інтеграція з MS Active Directory.
- Підтримка сервера баз даних MS SQL 2012 і вище.
- Підтримка сервера баз даних Azure SQL
- Підтримка ОС Windows 7 і новіших версій, macOS 10.10 і новіших версій
- Підтримка ОС Windows Server 2012 та вище.
- Інтеграція з Office 365
- Можливість налаштування консолі управління в залежності від потреб адміністратора.
- Можливість налаштовувати права доступу до звітів та налаштувань продукту, управління правами доступу адміністраторів.
- Прихований режим, включаючи приховування процесів і папок навіть для локального або адміністратора домену на кінцевій точці.

Захист системи від втручання:

- Захист від втручання у систему повинен бути активним для користувачів, локальних та доменних адміністраторів.

- Неможливість зупинки процесів, у випадку більш високих прав користувача, програма має оновити зупинені процеси або використовувати інший спосіб.

- Неможливість видалити програми без явного дозволу.

- Неможливість редагувати реєстр, компоненти системи та бібліотеки

DLL.

- Неможливість змінити налаштування з кінцевої точки.

- Забезпечення захисту в безпечному режимі.

- Функціональність повинна зберігатися в автономному режимі, тобто під час перебування поза мережею компанії, чи прямого підключення до мережі Інтернет.

- Можливість працювати з архівними записами.

- Рішення повинне підтримувати або бути в здатні забезпечити резервне копіювання власних компонентів, особливо записів і конфігурацій.

- Наявність менеджера бази даних. Можливість резервного копіювання, управління, огляд використаного простору бази. Створення задач для резервного копіювання. Підключення архівів до серверу для огляду інформації.

- Можливість за допомогою планувальника створювати архіви бази даних. Можливість підключення створених архівів за допомогою інтерфейсу серверу управління для перегляду збереженої інформації.

- Автоматичне повідомлення електронною поштою у випадку інцидентів, можливість змінювати рівень чутливості та специфікацію інциденту.

- Автоматичне генерування звітів на електронну пошту з можливістю повного коригування (обсяг інформації, список користувачів що відслідковуються, частота надсилання, отримувачі.)

- Можливість надсилати звіти в систему SIEM.

- Наявність веб консолі для отримання інформації про інциденти безпеки та відслідковування продуктивності роботи співробітників

- Контроль друку на локальних, мережевих та віртуальних принтерах. Можливість встановлення квот на друк, що дозволяє обмежити не цільове використання корпоративного обладнання

- Можливість завантаження файлу що спричинив інцидент

Загальні вимоги до аудиту безпеки:

- Детальна інформація про час запуску програмного забезпечення, а також про час активного використання. Використання категорій додатків для швидкої оцінки.

- Інформація про активний час, проведений на веб-сторінках, включаючи детальну інформацію про URL, протокол та заголовок незалежно від типу браузера. Наявність вбудованої категоризації веб-ресурсів.

- Можливість експорту звітів у XLS, PDF.

- ІМ програмне забезпечення, веб-поштовий клієнт:

- можливість відстеження даних, що надсилаються, незалежно від типу програми або сервісу

- Наявність вбудованих автоматичних щотижневих та щомісячних звітів про використання робочого часу.

E-mail:

- Підтримка POP3, IMAP, MAPI / Exchange протоколів, включаючи SSL-шифрування.

- MS Outlook, Thunderbird, IceWarp та ін. Клієнтська підтримка електронної пошти - це рішення дозволяє контролювати клієнти електронної пошти незалежно від типу програми.

Трафік даних:

- Детальна інформація про роботу з конфіденційними файлами, тобто хто відкрив файли, яке програмне забезпечення було використано для роботи з ними, збереження місцезнаходження, перейменування та видалення, зовнішні пристрої, електронна пошта та хмарне сховище, у тому числі, синхронізована папка на диску.

- Локальні операції з файлами - копіювання, переміщення, завантаження з Інтернету, FTP, видалення, створення, відкриття, включаючи ідентифікацію джерела та місця призначення - шлях, тип пристрою, унікальний ідентифікатор.

- Журналювання даних що друкуються

- Використання буферу обміну та знімків екрану

Активність кінцевої точки:

- Увімкнення/вимкнення кінцевої точки

- Авторизація/ вихід користувача

- Переключення ПК в режим сну і вихід з нього

Мережева активність:

- Обсяг відправлених / завантажених даних.

Загальні вимоги до захисту даних:

- Незалежність від програмного забезпечення, протоколу, включаючи зашифровані з'єднання

- Стійкість до обходу захисту системних файлів у випадку використання посилань на інші папки, включаючи символічні посилання та подібні технології.

- Можливість класифікації конфіденційних даних за додатком, за URL-адресою, за шляхом на диску або за змістом.

- Можливість використання сторонніх класифікаторів конфіденційної інформації

- Контроль доступу до локальних та мережевих папок, дисків, та хмарних сховищ

Шифрування даних:

- повнодискове шифрування, навіть для системних дисків

- Шифрування флеш-накопичувачів USB.

- Попередження витоку даних:

- Визначення категорії конфіденційних даних може обмежувати рух та роботу з даними - які медіаносії можна використовувати для передачі, які сайти можна використовувати для завантаження файлів, адреси електронної пошти, на які можна надсилати дані; яке програмне забезпечення може працювати з даними.

- Наявність режиму заборони, інформування та моніторингу

- Можливість встановлення політики для конкретних програм - визначення джерел (конкретні дані, доступ до зовнішніх пристроїв, мережа), які можуть бути використані додатком

- Можливість блокувати доступ користувачів до ресурсів в мережі інтернет використовуючи URL-адреси, домени, або вбудовані категорії веб- сайтів

- Можливість блокувати запуск прикладного ПЗ використовуючи вбудовані категорії або шлях виконуваного файлу

Контроль пристроїв:

- Глобальні обмеження щодо USB, firewire, карт пам'яті, LPT, COM, Bluetooth, CD, DVD, Blue-ray.

- Контроль підключення та використання зовнішніх пристроїв з можливістю створення дозволених та заборонених груп. Доступ до використання різних пристроїв таких як: usb-пристрої, CD/DVD, Bluetooth, LTP, Firewire і також інші NTFS файлові системи. Контроль доступу на рівні портів.

- Можливість встановлення режиму тільки для читання

- Журнал аудиту всіх зовнішніх пристроїв, що підключалися до системи в т.ч. монітори, клавіатури та комп'ютерні миші.

Інтеграція з мережевим обладнанням:

- Можливість інтеграції з мережевим обладнанням (інтернет та поштовими шлюзами), для забезпечення захисту від витоку даних на периметрі.

Орієнтовна вартість ліцензії на 90 об'єктів складає 99 000 гривень.

**Завідувач сектору інформаційних
технологій та захисту інформації
управління з організаційного
забезпечення Апеляційної палати
Вищого антикорупційного суду**



А. Калугін