**Обґрунтування**

**технічних та якісних характеристик, очікуваної вартості**

**Предмет закупівлі:** 4873 Пакети програмного забезпечення для забезпечення безпеки (Закупівля та впровадження інформаційної системи "Захищений віддалений користувач інформаційно-комунікаційної інфраструктури УДЦР")

**Технічні та якісні характеристики предмета закупівлі:**

Програмне забезпечення інформаційної системи «Захищений віддалений користувач інформаційно-комунікаційної інфраструктури УДЦР» має відповідати таким вимогам:

1. Мати можливість:

- інтеграції зі службою Windows Active Directory;

- збереження даних на серверах баз даних Microsoft SQL Server, а також Azure SQL;

- функціонування під управлінням операційних систем (далі – ОС) типу Microsoft Windows, Microsoft Windows Server, macOS;

- інтеграції із Office 365;

- використання технології «оптичного розпізнавання символів» (optical character recognition) для цілей перевірки контенту (даних);

- налаштування консолі управління в залежності від потреб адміністратора;

- налаштування різних права доступу;

- використання «прихованого режиму», включаючи можливість приховування «процесів» ПП 1 в ОС та каталогів ПП 1 в ОС для локального адміністратора, адміністратора домену, користувачів кінцевих точок;

- захисту від несанкціонованого втручання зі сторони користувачів кінцевих точок, а також доменних адміністраторів;

- відновлення «процесів» ПП 1 в ОС у випадку їх відключення;

- захисту від видалення без відповідного повноваження на таку дію;

- захисту внесення змін в «реестр» ОС в частині ПП 1, компонентів та бібліотек ПП 1;

- захисту від зміни налаштування зі сторони користувачів кінцевих точок;

- забезпечення захисту в «безпечному режимі»;

- функціонування в автономному режимі;

- роботи із архівними записами;

- забезпечувати резервне копіювання власних компонентів, записів, а також конфігурацій;

- резервного копіювання, управління, перегляду використаного простору, формування задач для резервного копіювання, а також можливість підключення архівів з метою перегляду інформації;

- автоматизації процесів створення архівів бази даних, підключення створених архівів за допомогою відповідного інтерфейсу призначеного для управління та перегляду такої інформації;

- налаштування функціоналу автоматичного повідомлення електронною поштою про виникнення інцидентів, а також можливість зміни рівня «чутливості» та специфіки інциденту;

- автоматичного формування звітів, які надсилаються електронною поштою із можливістю коригування обсягу інформації звіту, списку користувачів, які відслідковуються, частоти надсилання, списку отримувачів;

- надсилання звітів до «Security information and event management»;

- керування засобами «веб – консолі» та моніторингу інцидентів безпеки, а також відслідковування продуктивності роботи кінцевих користувачів;

- контролю друку на локальних, мережевих та віртуальних принтерах, а також можливість встановлення квот на друк;

- завантаження файлу, який спричинив спрацювання інциденту;

- налаштування та управління політиками доступу до «веб-ресурсів», комп’ютерних програм, а також їх категорій для кінцевих користувачів;

- інтеграції наявного інтерфейсу прикладного програмування зі службами звітності типу Power BI та/або Tableau;

- розгортання агентів моніторингу за допомогою групових політик Windows Active Directory або консолі «ESET PROTECT».

2. Забезпечувати аудит безпеки (звітність), в частині загальних вимог, електронної пошти, трафіку даних, а саме:

- детальне протоколювання (логування) інформації про час запуску програмного забезпечення, а також про час активного використання, використання категорій додатків для швидкої оцінки;

- протоколювання (логування) інформації про активний час, проведений на веб-ресурсах, включаючи детальну інформацію про адреси (URL), протоколу та заголовку незалежно від типу веб-браузера, наявність вбудованої категоризації веб-ресурсів;

- можливість експорту звітів у файли форматів XLS, PDF;

- протоколювання дій програмного забезпечення, веб-поштових клієнтів;

- відстеження даних, що надсилаються, незалежно від типу програмного забезпечення або сервісу, що забезпечує таке надсилання;

- можливість автоматичного формування щотижневого та щомісячного звітів про використання робочого часу;

- надсилання звітів із використанням протоколів POP3, IMAP, MAPI / Exchange, включаючи підтримку протоколу шифрування SSL;

- контроль MS Outlook, Thunderbird, Icewarp та ін;

- детальне протоколювання (логування) інформації про роботу з конфіденційними файлами, а саме хто відкривав файли, яке програмне забезпечення було використано для роботи з ними, збереження, місцезнаходження, перейменування та видалення, зовнішні пристрої, електронна пошта, або хмарне сховище, у тому числі синхронізований каталог (папка) на носії інформації;

- протоколювання інформації про «локальні» операції з файлами, а саме копіювання, переміщення, завантаження з мережі Інтернет, передача із до «FTP-ресурсу», видалення, створення, відкриття, а також інформацію про ідентифікацію джерела та місця призначення (шлях), тип пристрою, унікальний ідентифікатор;

- журналювання даних, що друкуються;

- протоколювання використання «буферу обміну» та «знімків екрану»;

- активності кінцевих точок, а саме увімкнення / вимкнення кінцевої точки, авторизація / вихід користувача, переключення комп’ютера в режим сну і вихід з нього, мережеву активність, обсяг відправлених / завантажених даних.

3. Забезпечувати захист даних, шифрування даних, попередження (протидія) витоку даних, контроль пристроїв, інтеграцію з мережевим обладнанням, а саме:

- захист даних незалежно від програмного забезпечення, протоколу, включаючи зашифровані з'єднання;

- стійкість до обходу захисту системних файлів у випадку використання посилань на інші каталоги (папки), включаючи символьні посилання та подібні технології;

- класифікацію конфіденційних даних за додатком, за «URL-адресою», за шляхом на носії інформації або за змістом;

- використання сторонніх класифікаторів конфіденційної інформації (метаданих), а саме із можливістю контролю доступу до локальних та мережевих каталогів (папок), носії інформації (дисків), хмарних сховищ, забезпечувати можливість дозволити певним кінцевим користувачам самостійно вказувати, які файли є конфіденційними;

- формування тіньової копії файлів.

- повнодискове шифрування, у тому числі системних дисків;

- шифрування земних носіїв інформації типу флеш-накопичувачів USB;

- обмеження роботи з даними (файлами) за визначеною категорією, в частині дозволу використання медіаносіїв для використання та передачі, дозволу використання певних «веб-ресурсів» для завантаження файлів, адрес електронної пошти, на які надсилати дані;

- режиму функціонування «заборона», «інформування», «моніторинг»;

- політику для конкретних комп’ютерних програм - визначення джерел (конкретні дані, доступ до зовнішніх пристроїв, мережа), які можуть бути використані;

- блокувати доступ користувачів до ресурсів в мережі Інтернет використовуючи «URL-адреси ресурсів», домени, вбудовані категорії веб-ресурсів;

- блокувати запуск прикладного програмного забезпечення використовуючи вбудовані категорії або шлях виконуваного файл;

- блокувати витік файлів конкретних розширень.

- застосування глобальних обмежень 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, використання різних пристроїв таких як: usb-пристрої, MTP, CD/DVD, Bluetooth, LTP, Firewire і також інші, контроль доступу на рівні портів;

- встановлення режиму «тільки для читання»;

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

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

4. Мати діючий експертний висновок у сфері технічного захисту інформації, який підтверджує його відповідність вимогам нормативних документів системи технічного захисту інформації в Україні та можливості його використання для забезпечення технічного захисту інформації, такий експертний висновок повинен бути зареєстрованим Адміністрацією Державної служби спеціального зв’язку та захисту інформації України.

5. Окремо, також, має бути поставлене програмне забезпечення яке:

- реалізує криптоалгоритми: ДСТУ 4145-2002; ДСТУ 7564:2014; ДСТУ 7624:2014;  ДСТУ ISO/IEC 18033-3:2015; ДСТУ ISO/IEC 14888-3:2019;

ДСТУ ISO/IEC 10118-3:2005; ДСТУ 11770-3:2015;

- здійснює генерацію випадкових послідовностей згідно із Додатком А до ДСТУ 4145-2002 ;

- має діючий експертний висновок Адміністрації Державної служби спеціального зв’язку та захисту інформації України за результатами державної експертизи в сфері криптографічного захисту інформації.

Також, мають бути надані послуги щодо впровадження програмного забезпечення системи «Захищений віддалений користувач інформаційно-комунікаційної інфраструктури УДЦР» та побудови комплексної системи захисту інформації в інформаційно-комунікаційній системі «Захищений віддалений користувач інформаційно-комунікаційної інфраструктури УДЦР».

**Очікувана вартість предмета закупівлі:**

Очікувана вартість предмета закупівлі: очікувана вартість визначена відповідно до процедур, які зазначені у примірній методиці визначення очікуваної вартості предмета закупівлі, введеної наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 №275 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі». На підставі аналізу аналогічних пропозицій учасників торгів на майданчику Prozorro, очікувана вартість становить 3 400 000 грн.

**Директор департаменту ІТ Сергій СИРОВЕЦЬ**

Виконав: Бондаренко В.І. т.422-85-81