НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ОБҐРУНТУВАННЯ

технічних та якісних характеристик закупівлі**,** розміру бюджетного призначення, очікуваної вартості предмета закупівлі

(оприлюднюється на виконання постанови КМУ № 710 від 11.10.2016 «Про ефективне використання державних коштів» (зі змінами))

Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб — підприємців та громадських формувань, його категорія: Національна академія внутрішніх справ.
03035, м. Київ, пл. Солом'янська, 1.
код за ЄДРПОУ – 08751177.
Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі й частин предмета закупівлі (лотів) (за наявності): Системи та пристрої нагляду та охорони (Код за ДК 021:2015 - 35120000-1 Системи та пристрої нагляду та охорони).

Вид та ідентифікатор процедури закупівлі: послуга, UA-2024-10-05-000304-a

Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі: 2786115,00 грн., з ПДВ. Визначення очікуваної вартості предмета закупівлі обумовлено статистичним аналізом загальнодоступної інформації про ціну предмета закупівлі на підставі затвердженої центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері публічних закупівель, примірної методики визначення очікуваної вартості предмета закупівлі, а саме: згідно з пунктом 1 розділу III наказу Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 із змінами.

Розмір бюджетного призначення: 2786115,00 грн., з ПДВ згідно з розрахунком до кошторису.

Обґрунтування технічних та якісних характеристик предмета закупівлі.

Термін надання послуг - До 08.11.2024 року

Характеристика об'єкту

Вимоги до комплексу

Вимоги до локальної мережі

Побудова локальної мережі:

Локальна мережа повинна бути побудована на базі структурованої кабельної системи, яка забезпечує швидкість передачі даних не менше 1 Гбіт/с. Тип кабелів мають бути використані мідні кабелі категорії cat 5e екрановані для горизонтальних з'єднань та оптоволоконні кабелі для магістральних з'єднань.

Встановлення серверних шаф:

Серверні шафи повинні відповідати стандартам IP20 (для внутрішнього встановлення) або IP55 (для зовнішнього встановлення).

Шафи повинні мати достатню місткість для розміщення всього запланованого обладнання. Шафи повинні бути обладнані активною системою охолодження для забезпечення належної температури всередині шафи. Потрібно забезпечити вільний потік повітря для охолодження обладнання.

Кабелі всередині серверних шаф повинні бути організовані таким чином, щоб забезпечити зручний доступ до обладнання, мінімізувати ризик перегріву та забезпечити належну вентиляцію.

Усі серверні шафи повинні бути належним чином заземлені для забезпечення безпеки експлуатації обладнання.

Встановлення патч-панелей та оптоволоконних панелей:

Патч-панелі повинні бути сумісними з кабелями категорії cat 5e (мідні) та відповідати стандартам для оптоволоконних з'єднань типу SC.

Оптоволоконні панелі повинні підтримувати з'єднання типу SC, Панелі повинні забезпечувати високу щільність портів для зручного розташування оптичних кабелів.

Патч-панелі та оптоволоконні панелі повинні бути встановлені у серверних шафах із дотриманням вимог щодо доступності та зручності підключення кабелів. Всі з'єднання повинні бути надійними та забезпечувати мінімальні втрати сигналу.

Всі порти на патч-панелях та оптоволоконних панелях повинні бути чітко промарковані. Необхідно забезпечити зручність ідентифікації з'єднань для полегшення технічного обслуговування.

Після встановлення патч-панелі та оптоволоконні панелі повинні бути протестовані для підтвердження їхньої працездатності. Результати тестування надаються замовнику.

Вимоги до системи контролю доступу

Система повинна повністю задовольняти вимогам до функціонування, описаним в даному технічному завданні, забезпечувати роботу 24 години на добу, 7 днів на тиждень, а також можливість оперативного отримання інформації про будь-які несправності або збої в роботі обладнання.

Система повинна дозволяти створювати складну і в теж час досить гнучку СКУД, використовуючи найбільш доцільне для кожного завдання обладнання, бути простою і зручною у впровадженні, використанні і адмініструванні. Система повинна мати модульну структуру, яка дозволила б нарощувати функціональність системи поступово, з урахуванням збільшення точок доступу, збільшенням чисельності персоналу або появі потреб у нових функціях .

Система повинна зберігати конфігурації, базу даних подій та користувачів при аварійному відключенні електроживлення, а також мати можливість автономної роботи, при втраті зв'язку між складовими частинами системи та сервером.

Система повинна забезпечувати безумовний захист інформації, яку вона обробляє або зберігає

Необхідно передбачити два режими роботи Системи - штатний і позаштатний. У штатному режимі, система повинна фіксувати всі перепустки та автоматично дозволяти чи блокувати доступ згідно з встановлених правил доступу чи розкладів. У позаштатному режимі (у випадку пожежі, надзвичайних подій, відключення електроживлення, інше) система повинна мати механізм аварійного розблокування проходу.

Виконавчі механізми та електронні пристрої, розміщені в зоні проходу мусять бути належного кліматичного виконання та залишатися працездатними при температурі від +5 до +40 градусів Цельсія. Всі первинні елементи системи повинні підтримувати електроживлення від мережі змінного струму 220В 50Гц, вторинні - 12В постійного струму. Система повинна

зберігати працездатність у випадку перебоїв в енергопостачанні протягом не менше однієї години.

В якості ідентифікаторів користувачів в системі повинні застосовуватися проксіміті карти, що представляють собою пластикову безконтактну картку-перепустку з унікальним ідентифікаційним кодом. Карта повинна мати велике число циклів зчитування, забезпечувати стабільну дистанцію зчитування не менше 30мм.

Обмін даними в системі (сервер, АРМ, контролери доступу) необхідно реалізувати за технологією Ethernet з використанням протоколу передачі даних TCP/IP. Контролери повинні працювати як в режимі зв'язку з центральним сервером, так і в автономному режимі у разі втрати зв'язку. Контролер повинний зберігати історію подій у внутрішній пам’яті, не менше 30000, з подальшою передачею даних на центральний сервер після відновлення зв'язку.

У Системі повинна бути передбачена можливість встановлення клієнтського місця ПЗ на АРМ оператора для можливості відображення подій, що відбуваються в системі відповідно до прав користувача, виданих адміністратором Системи для даного клієнтського місця.

Програмне забезпечення системи повинно бути захищене від несанкціонованого доступу. Всі спроби злому, перепрограмування, перезапису і інших видів саботажу повинні фіксуватися на центральному сервері і формуватися в звіті адміністратору Системи.

Гарантійний термін на обладнання системи (яке постачається в рамках даної закупівлі) повинен становити не менше 12 місяців.

Система повинна відповідати діючим будівельним, пожежним санітарним та іншим нормам, що забезпечує безпечні монтажні та налагоджувальні роботи, експлуатацію, обслуговування і сервісний ремонт Системи або її частин.

Вимога до функціональної частини системи контролю доступу

Система повинна виконувати наступні функції:

- ведення обліку виданих електронних перепусток співробітникам;
- створення розкладів доступу будь-якого рівня складності;
- ведення та перегляд історії змін інформації співробітника;
- перевірка прав доступу з урахуванням графіка роботи (обмеження доступу на територію підприємства в неробочий час);
- відображення на моніторі в реальному часі необхідної інформації про власника перепустки (в тому числі його фотографія), за яким відбувається прохід в даний момент;
- відображення у вигляді списку інформації про останні реєстраціях;
- управління виконавчими пристроями;
- автоматичне керування контролем доступу на підставі даних, що зберігаються в базі системи,
- управління пристроями контролю і управління доступом: робота в off-line режимі з контролерами доступу, швидке налаштування, попереднє налаштування існуючих пристроїв в Системі, а також додавання нових, настройка часу знаходження виконавчих пристроїв у відкритому стані, автоматичний контроль справності контролерів доступу і ліній зв'язку;
- час відгуку Системи при реєстрації ідентифікатора не повинна перевищувати дві секунди;
- збір інформації про відмітки в Системі;
- формування звітної документації, в тому числі обліку робочого часу;
- зберігати інформацію про події в системі не менше одного року.

Склад системи контролю доступу

Апаратні засоби, що використовуються в Системі:

1. Безконтактні ідентифікатори у кількості 1000 шт;
2. Персоналізатори для ідентифікаторів - настольний зчитувач з інтерфейсом USB;
3. Для обробки інформації від зчитувачів повинен використовуватися контролер доступу що відповідає наступним вимогам:

працює в IP мережах - Ethernet 100Mbit. Підтримка DHCP, DNS. Підключення до мережі - стандартний мережевий кабель (роз'єм RJ45);

Робота в складних, динамічно змінюваних комп'ютерних мережах (включаючи мережу Інтернет), через численні NAT. Не потребує додаткових налаштувань мережевого обладнання;

Розширена безпеку при роботі з IP: крипто і імітостойкость протоколу;

Підключення зчитувачів - два (2) порту Wiegand;

Незалежна пам'ять, не менше: - 250 тимчасових зон, 250 тижневих розкладів, 250 вихідних, підтримка плаваючих розкладів, 30000 постійних карток і 1000 тимчасових карток відвідувачів, 47000 записів в журналі події.

Входів - 8, з контролем по струму для підключення датчиків, кнопок та інше.;

Контроль АКБ і живлення - 2 окремі входи;

Виходів для управління зовнішніми пристроями - 4 типу «сухий контакт». Два реле (C NO NC) 24В 5А, два реле (C NO) 24В 1А;

Живлення - 12В;

Конфігурація мережевих налаштувань - через порт mini USB, або за допомогою процедури автоконфігурації.

4. Для обмеження доступу використовується наявний у замовника електомеханичні/привідни турнікети типу трипод:

Корпус та штанги із нержавіючої полірованої сталі;

Автиматизована функція опускання загородної штанги;

Можливість дістаційного керування за допомогою пульта (вхід, вихід, заблоковано,вільний прохід);

Живлення - 12В;

Споживана потужність Вт, не більше – 25;

Пропускна здатність в режимі однократного проходу, люд/хв не менше - 20;

Строк служби, років, не менше - 10;

Експлуатація за температури - від +5°С до +45°С та відносної вологості повітря не більше 95% при t=+25°С;

5. Для запеспечення вільного проходу у випадках надзвичайних сітуаций предбачити кнопку фізичного разблокування кожної точки доступу.

6. Програмно-апаратний комплекс СКУД повинен включати:

Операційну система Windows Server

Обов’язкова сумісність ПЗ СКУД з базами даних Microsoft SQL версії не нижче 2015.

Обладнання треба розмістити в приміщенні комендатури.

Вимоги до локальної мережі системи контролю доступу

1. В якості мережі передачі даних використовувати створену локальну мережу Ethernet (протокол передачі даних TCP / IP).

2. Окремі ділянки системи об’єднуються у єдину мережу, що розташовується у створеній локальній мережі. Для того, щоб виключити будь-яке втручання у діяльність системи зовнішніх факторів, кожна її ділянка підключена до міжмережевого екрану, який регулює та фільтрує обидва трафіка, як той, що виходить, так і той, що заходить до цієї ділянки. Завдяки застосованій схемі здійснюється повний контроль доступу до всіх ділянок мережі СКУД.

3. Вимоги до апаратного складу системи захисту.

a. Повинні бути застосовані механізми глибокої фільтрації та контролю трафіка (в тому числі IPS)

b. Повинна бути організована єдина консоль керування, з якої забезпечується можливість контролю кожного пристрою та керування ними

c. Обладнання, що використовується, повинно забезпечувати режими роботи «онлайн» (із включенням у розрив схеми та перенаправленням пакетів) та «прозорий» (без зміни трафіка)

d. Обладнання повинно мати спроможність генерації звітів про загрози, які виникали в процесі роботи

e. Обладнання повинно мати спроможність контролювати рівень загроз за встановленими критеріями та повідомляти уповноважених осіб за умови перевищення встановлених критеріїв.

Вимоги до програмного забезпечення системи контрою доступу

Програмне забезпечення СКУД повинно бути реалізовано з використанням сучасних технічних і програмних засобів, що забезпечують багатокористувацький доступ до інформації, зручність в експлуатації і сучасною функціональністю та інтеграцію з інформаційною інфраструктурою підприємства шляхом функціонального доповнення її елементів.

Система повинна мати трирівневу архітектуру: сервер баз даних (БД) - сервер додатків - сервер пристроїв, що забезпечує:

• невисокі вимоги до продуктивності робочих станцій і серверів;

• просте адміністрування та оновлення;

«Клієнт-серверна» архітектура системи повинна забезпечить можливість одночасної роботи в системі всіх користувачів на підприємстві. Кількість врахованих табельних номерів, підрозділів підприємства, професій, режимів змінності, причин неявок повинні відповідати фактичним параметрам підприємства.

Повинна бути передбачена можливість зміни кількості обладнання пунктів контролю та інсталяції додаткових програмних модулів в процесі експлуатації системи без доопрацювання її програмного забезпечення.

Програмне забезпечення повинно мати модульну структуру.

Функціонал програмного забезпечення повинен забезпечувати:

1. Управління персоналом:

a. Управління довідником підрозділів підприємства.

b. Управління довідником професій.

c. Управління довідником співробітників підприємства.

d. Управління довідником ідентифікаційних ознак (кодів, шаблонів ідентифікації).

e. Створення та редагування фотографічних даних працівників.

f. Управління довідником прийнятих, звільнених, переведених працівників.

g. Управління довідником режимів роботи.

2. Підготовка та персоналізація ідентифікаторів.

a. Зіставлення інформації про працівника і його ідентифікаційними ознаками.

b. Забезпечення як автоматичної (за допомогою персоналізаторів), так і ручний персоналізації ідентифікаторів.

3. Ведення обліку резервних ідентифікаторів.

a. Реєстрація персоналізації і повернення резервних ідентифікаторів.

b. Облік працівників підприємства, з різних причин користувалися резервними ідентифікаторами.

c. Облік причин використання резервних ідентифікаторів

4. Планування і коректування режимів доступу

a. Управління довідником режимів доступу.

b. Управління довідником інтервалів доступу для кожного з режимів.

5. Управління зонами доступу.

a. Управління довідником груп зон.

b. Управління довідником зон.

6.Управленіе пристроями контролю і управління доступом.

a. Управління довідником груп пристроїв.

b. Управління довідником пристроїв.

c. Робота з автономними (off-line) контролерами доступу.

d. Робота з мережевими (on-line) контролерами доступу.

e. Налаштування часу знаходження виконавчих пристроїв у відкритому стані.

f. Контроль за станом виконавчих пристроїв.

g. Автоматичний контроль справності контролерів доступу і ліній зв'язку.

7. Облік відвідувачів підприємства.

a. Управління довідником організацій.

b. Управління довідником разових пропусків.

c. Автоматичне анулювання одноразових перепусток за заданими параметрами.

d. Автоматичне формування довідника груп відвідувачів.

e. Автоматичне формування довідника відвідувачів.

f. Автоматичне формування довідника разових відвідувачів.

8. Збір інформації про відмітки.

a. Автоматичне управління контролем доступу на підставі даних, що зберігаються в базі системи.

b. Автоматична реєстрація всіх відміток у базі даних системи.

c. Автоматичне протоколювання поточних подій (дозвіл і відмова в доступі, збої і т.д.).

9. Управління доступом користувачів до ресурсів системи.

a. Управління довідником груп користувачів.

b. Управління довідником користувачів.

c. Управління правами груп користувачів.

d. Управління правами користувачів.

e. Ведення журналу роботи системи, що відображає всі зміни в базі даних, виконаних користувачами.

10. Формування звітної документації.

a. Контрольний звіт про процес реєстрації суб'єктів на контрольних пунктах.

b. Список відвідувачів.

c. Список власників ідентифікаторів.

d. Звіт по реєстраціях співробітників.

e. Звіт по реєстраціях відвідувачів.

f. Звіт про місцезнаходження співробітників і відвідувачів.

g. Список і зведення про знаходяться на території.

h. Список працівників, які мають непарні позначки.

i. Список працівників, які не мають позначок.

j. Список відзначалися на кожному контрольному пункті.

11. Модуль "Монітор охоронця"

a. Модуль "Монітор охоронця" дозволяє відстежувати всі події, що відбуваються в системі, в реальному режимі часу і виконує такі функції:

b. відображення реєстраційної інформації по співробітниках: дата і час реєстрації, прізвище, ім'я, по батькові та фотографія співробітника;

c. відображення реєстраційної інформації по відвідувачах: дата і час реєстрації, прізвище, ім'я та по батькові відвідувача;

d. відображення у вигляді списку інформації про останні реєстраціях;

e. управління виконавчими пристроями: одиночний прохід, вільний прохід, блокування проходу.

12. Модуль «Облік робочого часу»

Точність обліку робочого часу - 1 хвилина. Сумарні величини відпрацьованого часу по підприємству або підрозділу округлюються до 1 години.

1. Планування і коригування графіків виходів і вихідних днів.

a. Управління довідником графіків виходів підрозділів

b. Управління довідником графіків виходів груп працівників

c. Управління довідником індивідуальних графіків виходів працівників
d. Автоматичне планування графіка виходів за фактичними відмітками
e. Автоматичне планування графіків виходів на підставі шаблонів.
f. Призначення шаблонів графіків виходів (за замовчуванням) для спрощеного планування графіка виходів співробітників
g. Управління довідником інтервалів доступу для кожного з графіків
h. Створення та редагування шаблонів графіків виходів
i. Контроль коректності складання графіків виходів

2. Коригування параметрів співробітників списком.

Ручне введення відміток.

a. Забезпечення можливості роботи без обладнання (ручне введення відміток)
b. Контроль і коригування непарних відміток (як в ручному, так і в автоматичному режимі)

3. Облік причин відсутності.

a. Управління списком причин неявок
b. Реєстрація передбачуваних і фактичних причин неявок

4. Облік цілодобових режимів роботи.

a. Управління кордонами початку / кінця зміни, приходу / відходу, пізнього приходу / раннього відходу
b. Управління кордонами нічного часу, перерви, параметрами відпрацьованого часу

5. Управління нормативно-довідковою інформацією.

a. Управління довідником фіксованих подій
b. Перегляд довідника державних свят і святкових днів

6. Формування звітної документації (в тому числі можливість відображення аналітики через Power BI):

a. Можливість зміни і налаштування процедури розрахунку підсумкових відомостей.
b. Оперативні документи.

7. Списки:

a. Список співробітників, що не з'явилися по поважним запланованим причинам.
b. Список, що не з'явилися з невідомих причин.
c. Список працівників із заданою причиною неявки.
d. Облік порушень трудової дисципліни.
e. Список тих, хто відпрацював зміну.
f. Список працівників, які мають непарні позначки.
g. Список працівників, які не мають позначок.
h. Список прийнятих працівників за період
i. Список звільнених працівників за період
j. Список переведених працівників за період
k. Список режимів змінності
l. Список співробітників з режимами змінності
m. Список співробітників без режимів змінності
n. Список співробітників без запланованих змін

8. Документи обліку робочого часу:

a. Книга обліку понаднормових годин.
b. Облік робочого часу (6 форм)
c. Облік робочого часу. Знаходження в зоні
d. Облік співробітників, що запізнилися

9. Аналітичні документи:

a. Список співробітників з режимами змінності
b. Звіт про відпрацьований час
c. Відпрацьований час в розрізі підрозділів
d. Графік виходів
e. Відхилення від робочих графіків
f. Використання службових потреб

g. Журнал обліку ручних відміток

Вимоги до системи відеоспостереження

Система відеоспостереження повинна забезпечувати безперервний моніторинг визначених зон з можливістю запису та зберігання відеоінформації протягом не менше 30 днів.

Система повинна бути інтегрована з існуючою мережею та мати можливість віддаленого доступу через веб-інтерфейс або мобільний додаток.

Все обладнання повинно відповідати стандартам безпеки та мати сертифікати відповідності.

Камери відеоспостереження

- Тип камер: IP-камери з підтримкою протоколу ONVIF.
- Роздільна здатність камер: не менше 4 МП.
- Наявність інфрачервоного підсвічування для роботи в умовах недостатнього освітлення, дальність підсвічування не менше 30 метрів.

Відеореєстратори (NVR)

- Підтримка не менше 32 каналів відеозапису.
- Мінімальна роздільна здатність запису: 4К.
- Обсяг жорсткого диска для зберігання даних: не менше 8 ТБ з можливістю розширення.
- Можливість підключення додаткових зовнішніх накопичувачів для резервного копіювання.

Програмне забезпечення

- Програмне забезпечення для керування відеоспостереженням повинно мати зручний інтерфейс для перегляду відео в реальному часі, управління камерами та пошуку відеозаписів.
- Підтримка зберігання архівних відеозаписів з можливістю пошуку за датою, часом, подіями.
- Вимоги до монтажу та введення в експлуатацію

Усі роботи з встановлення обладнання повинні проводитися з урахуванням норм безпеки.

Система повинна бути змонтована та введена в експлуатацію з урахуванням усіх технічних вимог та побажань замовника.

Необхідно провести навчання персоналу замовника для роботи з системою відеоспостереження.