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): Комп'ютерне обладнання (Код за ДК 021:2015 – 30230000-0 Комп'ютерне обладнання)

Вид та ідентифікатор процедури закупівлі: UA-2024-04-03-009537-a

Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі: 4 249 420,00 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 ІІІ наказу Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 із змінами.

Розмір бюджетного призначення: 4 249 420,00 грн. з ПДВ згідно з розрахунком до кошторису.

Обґрунтування технічних та якісних характеристик предмета закупівлі.

Термін постачання — **До 01.05.2024 року.**
Придбання комп'ютерного обладнання здійснюється відповідно до наявної потреби для забезпечення належної підготовки фахівців у сфері кримінального аналізу за затвердженими професійними програмами. Оновлення комп'ютерної техніки є важливою складовою реалізації проекту під умовно назвою «Потєрь.нєт», запровадженого Міністерством внутрішніх справ спільно з Національною поліцією України. Сучасне комп'ютерне обладнання дасть можливість модернізувати матеріально-технічну базу академії; створити належні умови для якісного виконання освітніх процесів, зокрема для підготовки фахівців у сфері кримінального аналізу; підвищити рівень спроможності працівників сектору безпеки використовувати методи й інструменти кримінального аналізу для ефективного виконання покладених на них завдань з огляду на умови воєнного стану. Якісні та технічні характеристики заявленої кількості техніки визначені з урахуванням реальних потреб НАВС та оптимального співвідношення ціни та якості.

№ п/п	Характеристика товару	Од. виміру	Кіль-кість
1	**<u>Багатофункціональний пристрій:</u>** Функції: чорно-білий друк/копіювання/сканування/факс Технологія друку - лазерна Тип принтера - монохромний Максимальний формат носія друку - А4 Максимальна продуктивність на місяць (А4), не менше - 15 000 стор. Швидкість друку (чорно-білий, звичайна якість, А4), не менше - 20 стор. за хв. Час виходу першої сторінки під час друку, не більше - 8,5 сек. Якість друку (чорно-білий, найвища якість), не менше - 1200×1200 dpi Потужність процесора, не менше - 600 МГц Об'єм пам'яті (стандартний), не менше - 128 Мб Ємність основного лотка у стандартній комплектації, не менше - 150 аркушів Ємність обхідного лотка у стандартній комплектації, не менше - 1 аркуша Ємність вихідного лотка, не менше - 100 аркушів Інтерфейси у стандартній комплектації USB 2.0, Ethernet, Wi-Fi b/g/n Щільність носіїв, не гірша - 60-163 г/м2 Якість копіювання (чорно-біла, звичайна якість), не менше - 600×600 dpi Дозвіл сканування (оптичний), не менше - 600×600 dpi Вага апарату, не більше - 9 кг Потужність в режимі роботи, не більше - 320 Вт Оригінальний картридж із стандартним ресурсом друку від виробника Гарантія виробника: не менше 12 місяців	шт	40
2	**<u>Програмно-апаратний комплекс для відео монтажу та обробки відеоматеріалів (моноблок):</u>** Процесор: максимальна тактова частота - не менше ніж 4,4 GHz. кількість фізичних ядер: не менше ніж 12; кількість потоків: не менше ніж 16; обсяг кеш-пам’яті: не менше 12 MB	шт	40

	Корпус: Форм-фактор – моноблок Оперативна пам'ять: Об'єм пам'яті - не менше ніж 16 GB; тип пам'яті - не гірше ніж DDR4 3200 Mhz; Слоти розширення: Не менше ніж 1 х M.2 для SSD накопичувачів, 1 х M.2 для WLAN Накопичувач: Тип SSD, об’ємом пам’яті не менше ніж 512 GB Графічний адаптер: Інтегрований, не гірше Intel Iris Xe Graphics Бездротовий мережевий інтерфейс: Інтегрований модуль WI-FI - не гірше Wi-Fi 6E (802.11ax/ac/a/b/g/n) Мережевий адаптер: Інтегрований з підтримкою стандарту 1000BASE-T. Порти вводу-виводу: Не менше ніж 3 порти USB 3.X Type-A; Не менше ніж 1 порт USB 2.0 Type-A; Не менше ніж 1 порт USB 3.2 Type-C; Не менше ніж 1 порт HDMI; Не менше 1 х LAN (RJ-45); Не менше ніж 1 х Audio порт (комбінований) Мультимедіа: Вбудована веб-камера, не гірше ніж 5МП; мікрофон; стереодинаміки Блок живлення: Зовнішній адаптер потужністю не більше 65 Вт. Програмне забезпечення: Операційна система: не гірше ніж Microsoft® Windows® 11Pro мова інтерфейсу українська, предінстальована. Клавіатура: Стандартна, з окремим блоком клавіш для набору цифр; латинсько-кирилична розкладка, тип інтерфейсу – USB. Від виробника моноблоку Маніпулятор типу "миша":		

	Технологія - оптична; тип підключення - USB-інтерфейс; кількість кнопок - щонайменше 3: ліва, права, колесо-кнопка для скролінгу. Від виробника моноблоку Монітор: Розмір діагоналі: Не менше ніж 23.8” Тип панелі: Не гірше ніж IPS або аналог Покриття екрану: антиблікове Роздільна здатність: Не гірше ніж 1920 x 1080 (Full HD) Гарантія виробника: не менше 12 місяців Антивірусне програмне забезпечення з характеристиками не гірше: <u>Вимоги до рішення для захисту робочих станцій під управління несерверних ОС:</u> 1. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ. 2. Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп’ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання. 3. Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем. 4. Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо. 5. Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення. 6. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в ОС. 7. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування. 8. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи. 9. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.		

	10. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI. 11. Забезпечення антивірусного захисту в режимі реального часу. 12. Використання евристичних технологій власної розробки під час сканування. 13. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 14. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду. 15. Можливість сканування файлів під час запуску ОС. 16. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін. 17. Сканування комп'ютера у неактивному стані. 18. Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень. 19. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування 20. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення. 21. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо. 22. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware). 23. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами. 24. Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп’ютер від шкідливих програм і небажаної активності. 25. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру. 26. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі. 27. Автоматична антивірусна перевірка змінних носіїв. 28. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження.		

	29. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою. 30. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв. 31. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену. 32. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв. 33. Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі. 34. Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware». 35. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах. 36. Перевірка дійсності та цілісності сертифікатів SSL-трафіку. 37. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим . 38. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер. 39. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет" 40. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості ПЗ та надання докладнішої інформації про ідентифікатори CVE. 41. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання. 42. Регламентне оновлення вірусних баз не менше 24 разів за добу. 43. Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет. 44. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок. 45. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.		

	46. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею. 47. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну. 48. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень. 49. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС. 50. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання. 51. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі. 52. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час. 53. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання. 54. Локальне зберігання журналів на робочих станціях. 55. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми. 56. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій. 57. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. 58. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом. 59. Можливість захисту паролем параметрів рішення для захисту кінцевої точки. 60. Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі. 61. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності. 62. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.		

	63. Можливість крім основного вказати резервні сервери адміністрування. 64. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову. 65. Підтримка ОС: Microsoft Win 11, Win 10, 8.1, 8, 7 (SP1+KB). <u>Вимоги до рішення для захисту робочих станцій під управління серверних ОС:</u> 1. Підтримка ОС: Microsoft Win. Server: 2022, 2019, 2016, 2012R2, 2012, 2008(R2 SP1), Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2); Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15. 2. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи. 3. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 4. Сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах. 5. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду. 6. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації. 7. Можливість сканування файлів під час запуску ОС. 8. Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами. 9. Сканування комп'ютера у неактивному стані. 10. Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень. 11. Автоматична антивірусна перевірка змінних носіїв. 12. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою. 13. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows. 14. Наявність системи виявлення вторгнень (HIPS), яка захищає комп’ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил		

	для контролю запущених процесів, використовуваних файлів та розділів реєстру. 15. Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень. 16. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес. 17. Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим. 18. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж). 19. Регламентне оновлення вірусних баз не менше 24 разів за добу. 20. Можливість крім основного вказати резервні сервери адміністрування. 21. Наявність механізму контролю за актуальністю оновлень ОС. 22. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання. 23. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми. Можливість планування завдань, які запускатимуться одноразово, періодично та за умови виникнення конкретних подій. 24. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. 25. Можливість роботи в кластерах як домена так і робочої групи. 26. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування. 27. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів. 28. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.		

	29. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ. 30. Можливість захисту від зміни параметрів антивірусного ПЗ паролем. 31. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому. <u>Вимоги до інструменту віддаленого управління антивірусними рішеннями:</u> 1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури. 2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати централізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам. 3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 5. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно. 6. Віддалена інсталяція користувальницького програмного забезпечення. 7. Можливість віддаленого видалення встановленого користувальницького ПЗ. 8. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac 9. Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій командного рядка на клієнтському комп'ютері, старт оновлення операційної системи клієнтського комп'ютера. 10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac з попередньо встановленими настройками конфігурації, що дає можливість експортувати інсталяційні пакети для розгортання повноцінного антивірусного захисту на кінцевих точках в ізольованій мережі, а також на кінцевих точках, що потребують захисту, але тимчасово не мають з'єднання з сервером адміністрування. 11. Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів, груп комп'ютерів на сервері адміністрування, що дає можливість надати різні права доступу для регіональних системних адміністраторів розгалуженої системи антивірусного захисту.		

	12. Можливість аутентифікувати адміністраторів ERA за допомогою груп безпеки AD. 13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління. 14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування. 15. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів. 16. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань. 17. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю. 18. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик. 19. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування. 20. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів. 21. Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту. 22. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL. 23. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM. 24. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів. 25. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу. 26. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів. 27. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом. 28. Використання незалежного агенту, який дає можливість здійснювати віддалене управління антивірусним продуктом на кінцевих точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи.		

	29. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором. 30. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях 31. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту. 32. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів. 33. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування). 34. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу 35. Можливість встановлення серверу адміністрування на ОС Windows та Linux. 36. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії. 37. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому. 38. Можливість встановлення агенту управління на ARM64 процесорах. 39. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям. 40. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії. Термін підписки антивірусної програми: не менше 12 місяців		
3	**<u>Програмно-апаратний комплекс для відео монтажу та обробки відеоматеріалів (ноутбук):</u>** Процесор: не менше ніж 10 фізичних обчислювальних ядра; не менше 12 МБ кеш пам’яті третього рівня; підтримка технології Turbo Boost Technology із можливістю роботи на частоті не менше 4.4 GHz; підтримка технології HyperThreading або її аналог; рік випуску процесору повинен бути – не раніше 2022 року. Оперативна пам'ять: об’єм не менше 16GB DDR4; частота не нижче 3200 MHz; можливість збільшення об’єму оперативної пам'яті до 32 GB;	шт	60

	Накопичувач: тип накопичувача – SSD PCIe NVMe формату M.2; об`єм накопичувача - не менше 512 GB; Відеокарта: інтегрована Екран: діагональ не менше 15,6 дюймів; не гірше IPS з антибліковим покриттям; підтримка роздільної здатності не гірше FHD 1920x1080 точок; Порти вводу/виводу: не менше 3 портів USB Type-A версії не нижче USB 3.2; не менше 1 порт USB Type-C із підтримкою стандарту Thunderbolt 4.0 з можливістю заряджання пристрою та передача відеосигналу. універсальний аудіороз'єм під штекер TRS 3.5 мм; не менше 1 HDMI порт не гірше 1.4; не менше 1 кард-рідер; (всі порти повинні бути інтегровані в корпус, без додаткових адаптерів) Мережа: бездротова мережа WiFi з підтримкою стандартів не менш ніж 802.11ax; наявність Bluetooth з підтримкою стандарту 5.2; RJ-45 з швидкістю 100/1000 Мбіт/с; Пристрої вводу/виводу: вологозахисна клавіатура, інтегрована у корпус з цифровим блоком; латинсько-кирилична, з нанесеними виробником літерами латинського (US International) та українського алфавітів; інтегровані мікрофон та динаміки; Веб камера: обов’язкова наявність вбудованої камери з роздільною здатністю відео не гірше 720p та захисною шторкою; Живлення: вбудований акумулятор ємністю не менше 50 ватт-год; зовнішній блок живлення потужністю не менше 45Вт; Безпека: обов’язкова наявність апаратного модулю TPM 2.0; наявність слоту для замка безпеки;		

	Операційна система: попередньо встановлена без активації ОС Microsoft Windows 11 Pro (64Bit, українська редакція) на виробництві; Розміри: вага не більше 1,7 кг; Гарантійний строк: Гарантія виробника не менше 12 місяців Антивірусне програмне забезпечення з характеристиками не гірше: Вимоги до рішення для захисту робочих станцій під управління несерверних ОС: 1. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ. 2. Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп'ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання. 3. Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем. 4. Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо. 5. Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення. 6. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в ОС. 7. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування. 8. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.		

	9. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС. 10. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI. 11. Забезпечення антивірусного захисту в режимі реального часу. 12. Використання евристичних технологій власної розробки під час сканування. 13. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 14. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду. 15. Можливість сканування файлів під час запуску ОС. 16. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін. 17. Сканування комп'ютера у неактивному стані. 18. Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень. 19. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування 20. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення. 21. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо. 22. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware). 23. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами. 24. Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп’ютер від шкідливих програм і небажаної активності.		

	25. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру. 26. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі. 27. Автоматична антивірусна перевірка змінних носіїв. 28. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження. 29. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою. 30. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв. 31. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену. 32. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв. 33. Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі. 34. Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware». 35. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах. 36. Перевірка дійсності та цілісності сертифікатів SSL-трафіку. 37. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим . 38. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер. 39. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"		

	40. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості ПЗ та надання докладнішої інформації про ідентифікатори CVE. 41. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання. 42. Регламентне оновлення вірусних баз не менше 24 разів за добу. 43. Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет. 44. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок. 45. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне. 46. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею. 47. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну. 48. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень. 49. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС. 50. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання. 51. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі. 52. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час. 53. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання. 54. Локальне зберігання журналів на робочих станціях. 55. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка		

	стану системи, перевірка комп'ютера, оновлення вірусних баз та модулів програми. 56. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій. 57. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. 58. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом. 59. Можливість захисту паролем параметрів рішення для захисту кінцевої точки. 60. Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі. 61. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності. 62. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача. 63. Можливість крім основного вказати резервні сервери адміністрування. 64. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову. 65. Підтримка ОС: Microsoft Win 11, Win 10, 8.1, 8, 7 (SP1+KB). Вимоги до рішення для захисту робочих станцій під управління серверних ОС: 1. Підтримка ОС: Microsoft Win. Server: 2022, 2019, 2016, 2012R2, 2012, 2008(R2 SP1), Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2); Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15. 2. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи. 3. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку. 4. Сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.		

	5. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду. 6. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації. 7. Можливість сканування файлів під час запуску ОС. 8. Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами. 9. Сканування комп'ютера у неактивному стані. 10. Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень. 11. Автоматична антивірусна перевірка змінних носіїв. 12. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою. 13. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows. 14. Наявність системи виявлення вторгнень (HIPS), яка захищає комп’ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру. 15. Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень. 16. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес. 17. Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим. 18. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).		

	19. Регламентне оновлення вірусних баз не менше 24 разів за добу. 20. Можливість крім основного вказати резервні сервери адміністрування. 21. Наявність механізму контролю за актуальністю оновлень ОС. 22. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання. 23. Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп'ютера, оновлення вірусних баз та модулів програми. Можливість планування завдань, які запускатимуться одноразово, періодично та за умови виникнення конкретних подій. 24. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. 25. Можливість роботи в кластерах як домена так і робочої групи. 26. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування. 27. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів. 28. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом. 29. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ. 30. Можливість захисту від зміни параметрів антивірусного ПЗ паролем. 31. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому. Вимоги до інструменту віддаленого управління антивірусними рішеннями: 1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.		

	2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати централізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам. 3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux. 5. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно. 6. Віддалена інсталяція користувальницького програмного забезпечення. 7. Можливість віддаленого видалення встановленого користувальницького ПЗ. 8. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac 9. Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій командного рядка на клієнтському комп'ютері, старт оновлення операційної системи клієнтського комп'ютера. 10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac з попередньо встановленими настройками конфігурації, що дає можливість експортувати інсталяційні пакети для розгортання повноцінного антивірусного захисту на кінцевих точках в ізольованій мережі, а також на кінцевих точках, що потребують захисту, але тимчасово не мають з'єднання з сервером адміністрування. 11. Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів, груп комп'ютерів на сервері адміністрування, що дає можливість надати різні права доступу для регіональних системних адміністраторів розгалуженої системи антивірусного захисту. 12. Можливість аутентифікувати адміністраторів ERA за допомогою груп безпеки AD. 13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.		

	14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування. 15. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів. 16. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань. 17. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю. 18. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик. 19. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування. 20. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів. 21. Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту. 22. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL. 23. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM. 24. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів. 25. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу. 26. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів. 27. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом. 28. Використання незалежного агенту, який дає можливість здійснювати віддалене управління антивірусним продуктом на кінцевих		

	точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи. 29. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором. 30. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях 31. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту. 32. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів. 33. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування). 34. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу 35. Можливість встановлення серверу адміністрування на ОС Windows та Linux. 36. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії. 37. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому. 38. Можливість встановлення агенту управління на ARM64 процесорах. 39. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям. 40. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії. Термін підписки антивірусної програми: не менше 12 місяців		