ВИЩИЙ АНТИКОРУПЦІЙНИЙ СУД

НАКАЗ

06 грудня 2024 року Київ № 35-о

**Про затвердження
Положення про порядок
використання ресурсів локальної
комп'ютерної мережі у
Вищому антикорупційному суді**

З метою забезпечення правильного та ефективного використання в роботі комп'ютерного устаткування, ресурсів мережі Інтернет, електронної пошти, а також умов зберігання інформації та її розповсюдження

НАКАЗУЮ:

1. Затвердити Положення про порядок використання ресурсів локальної комп'ютерної мережі у Вищому антикорупційному суді, що додається.

2. Визнати такими, що втратили чинність, накази Вищого антикорупційного суду:

1) від 05 листопада 2019 року № 103 «Про затвердження Положення про порядок використання ресурсів локальної комп'ютерної мережі у Вищому антикорупційному суді»,

2) від 19 листопада 2020 року № 56-а «Про внесення змін у додатки до Положення про порядок використання ресурсів локальної комп'ютерної мережі у Вищому антикорупційному суді»;

3) від 27 вересня 2023 року № 19-а «Про внесення змін у додатки до Положення про порядок використання ресурсів локальної комп'ютерної мережі у Вищому антикорупційному суді».

3. Управлінню документообігу та організаційного забезпечення (Сівошко Ф.С.) довести цей наказ до відома суддів і працівників апарату Вищого антикорупційного суду.

4. Контроль за виконанням цього наказу залишаю за собою.

Керівник апарату **Богдан КРИКЛИВЕНКО**

ВНУТРІШНІ ВІЗИ:

Начальник управління інформаційних технологій та захисту інформації Олександр ГРАЇЦЬКИЙ

В.о начальника відділу правового забезпечення Олеся ДОЛЯ

Завідувач сектору запобігання та виявлення корупції Ксенія ГРОДЗИНСЬКА

ЗАТВЕРДЖЕНО
Наказ Вищого антикорупційного суду
від 16 грудня 2024 року № 35-о

ПОЛОЖЕННЯ
про порядок використання ресурсів локальної комп'ютерної мережі у Вищому антикорупційному суді

Положення про порядок використання ресурсів локальної комп'ютерної мережі у Вищому антикорупційному суді як суді першої інстанції (далі - Положення) визначає порядок підключення до локальної комп'ютерної мережі, порядок і права доступу до інформаційних ресурсів, містить необхідні вимоги щодо забезпечення спільної роботи в локальній комп'ютерній мережі, збереження інформації користувачів мережі і дотримання прав на її розповсюдження.

Дотримання цього Порядку необхідне для правильного функціонування мережі, підтримки і поглиблення інтеграції комп'ютерної мережі в мережу Інтернет, а також з іншими мережами.

Цей Порядок є обов'язковим для ознайомлення і дотримання кожним із користувачів комп'ютерної мережі.

I. Основні терміни

1. Мережа – локальна комп'ютерна мережа, розташована в приміщеннях Вищого антикорупційного суду як суду першої інстанції (далі - Суд) (сукупність комп'ютерів, кабельна система, сукупність мережевих адаптерів, активного мережевого обладнання, що працює під управлінням мережевих операційних систем і прикладного програмного забезпечення), до якої підключені судді та працівники апарату Суду, а також працівники, що віддалено підключені через мережу Інтернет, комп'ютери і комп'ютерні мережі інших установ і організацій, які виконують спільні із Судом завдання.

2. Адміністратор – відповідальний працівник Суду (працівник управління інформаційних технологій та захисту інформацій, який відповідає за роботу системного адміністратора або структурний підрозділ), що здійснює адміністрування серверів і робочих станцій, а також проектування і розвиток Мережі.

3. Користувач – користувач комп'ютера, підключеного до Мережі.

4. Робоча станція/комп'ютер – комп'ютер, встановлений у Суді та призначений для виконання Користувачем службових обов'язків.

II. Загальні положення

1. З метою забезпечення нормального функціонування Мережі Користувач зобов'язаний дотримуватися вимог цього Положення, відповідально використовувати ресурси Мережі, із повагою до їх власників та з дотриманням вимог чинного законодавства України, а також неухильно слідувати рекомендаціям Адміністратора.

2. При користуванні Мережею забороняється:

1) здійснювати пошкодження, знищення або фальсифікацію інформації, створеної іншими користувачами;

2) здійснювати будь-які види атак на ресурси Мережі, а також порушувати нормальну роботу мережевих служб і мережевого устаткування;

3) розповсюджувати інформацію, заборонену чинним законодавством України або яка не відповідає морально-етичним нормам суспільства, а також розсилати повідомлення з

метою погрожування, введення в оману, розповсюдження дезінформації та вчинення деструктивного інформаційного впливу;

4) здійснювати масове (більше п'яти повідомлень одному абоненту) надсилання електронних, текстових та/або мультимедійних повідомлень, не пов'язаних із службовою діяльністю, без попередньої згоди одержувачів на їхні адреси електронної пошти або кінцеве (термінальне) обладнання (спам);

5) використовувати надані ресурси із дотриманням принципів добросовісності та відповідальності.

3. Порушення вимог цього Положення може призвести до відключення Користувача від Мережі. Відключення може бути тимчасовим або умовно безстроковим, що відновлюється після вивчення та усунення причин відповідного порушення. Рішення про строк відключення залежить від суті вчиненого порушення та його наслідків.

4. Присутність Користувача в Мережі або його доступ до певних ресурсів Мережі можуть бути припинені/тимчасово зупинені за власним бажанням Користувача, у разі відсутності Користувача на робочому місці або з інших причин (необхідно завчасно повідомити про це Адміністратора в письмовій формі за попереднім погодженням безпосереднього керівника).

5. Управління Мережею здійснює Адміністратор, виконуючи роботи щодо супроводу і розвитку Мережі, підключення до Мережі, припинення доступу до Мережі, здійснення контролю використання ресурсів Мережі її користувачами.

III. Відповідальність, права і обов'язки Адміністратора

1. Адміністратор несе відповідальність за:
1) функціонування Мережі в цілому;
2) функціонування сервісів Мережі;
3) порушення функціонування Мережі у зв'язку з некоректним управлінням маршрутизацією та базовими мережевими сервісами.

2. Адміністратор зобов'язаний:
1) обмежити доступ співробітників і сторонніх відвідувачів до приміщень, в яких встановлені сервери і комутаційне устаткування Мережі;
2) забезпечити контроль структури Мережі;
3) здійснювати організаційні (контроль за дотриманням правил користування комп'ютерною технікою) та технічні (регулярна зміна мережевих паролів, відстеження запуску і припинення використання програмного забезпечення, що порушує нормальну працездатність Мережі та її безпеку, а також комп'ютерів в ній) заходи для недопущення/припинення несанкціонованого підключення до Мережі із зовнішніх мереж, а також із комп'ютерів Мережі;
4) здійснювати керівництво роботами, пов'язаними з впровадженням нових технологій і розвитком Мережі;
5) проводити заходи щодо забезпечення безпеки в Мережі;
6) подавати пропозиції про необхідність придбання нових ліцензійних комп'ютерних програм, забезпечувати отримання необхідних комп'ютерних програм, що розповсюджуються на безоплатній основі, та проводити їх інвентаризацію;
7) надавати Користувачам консультаційну допомогу з питань використання ресурсів Мережі.

3. Адміністратор має право:
1) відключати Мережу, якщо зафіксовано активність шкідливого програмного забезпечення, до усунення останньої;
2) частково або повністю відсторонювати Користувачів, які допустили порушення вимог цього Положення від використання Мережі;
3) приймати рішення щодо адміністративних питань взаємодії з користувачами Мережі.

IV. Права і обов'язки Користувача

1. Користувач має право:

1) на доступ до всіх ресурсів Мережі, відповідно до вимог цього Положення та з урахуванням посади та посадових обов'язків Користувача, що відображено в заповненій формі (додаток 1 до цього Положення);

2) надавати Адміністратору зауваження та пропозиції щодо роботи Мережі;

3) звертатися за довідковою інформацією і консультацією до Адміністратора.

2. Користувач зобов'язаний:

1) використовувати всі ресурси Мережі із дотриманням принципів добросовісності та відповідальності;

2) виконувати вказівки й рекомендації Адміністратора в межах вимог Положенням;

3) під час роботи з комп'ютерною технікою дотримуватися вимог інструкцій з охорони праці;

4) забезпечити нерозголошення ідентифікаційної інформації, яка використовується для доступу до ресурсів Мережі;

5) запобігати проявам несанкціонованого використання ресурсів Мережі. У разі виявлення таких спроб Користувач зобов'язаний поінформувати про це Адміністратора;

6) використовувати антивірусні програмні засоби, встановлені Адміністратором;

7) дотримуватися законодавства з питань правової охорони комп'ютерних програм та використовувати комп'ютерні програми в обсязі, формі, способом, визначеними в ліцензії або в ліцензійному договорі, або в іншому договорі щодо розпорядження майновими правами інтелектуальної власності.

3. Користувачу забороняється:

1) самостійно відкривати корпуси комп'ютерної техніки;

2) самостійно проводити ремонт або технічне обслуговування комп'ютерної техніки;

3) самовільно змінювати місце розташування та спосіб підключення Робочої станції до Мережі;

4) самовільно підключати до комп'ютерної техніки та використовувати додаткове периферійне обладнання, що має фізичну адресу (MAC-адресу – радіо-модеми, Wi-Fi-карти, Bluetooth-адаптери, мережеві карти тощо);

5) змінювати конфігурацію системних файлів, мережевих налагоджень;

6) надавати загальний доступ до комп'ютерної бездротової (Wi-Fi) мережі;

7) самостійно встановлювати і видаляти програмне забезпечення, використовувати будь-яке стороннє програмне забезпечення, ігрові та розважальні програми;

8) запрошувати сторонніх осіб без попереднього погодження з Адміністратором для виконання робіт, визначених підпунктами 1-7 пункту 3 розділу 4 Положення;

9) здійснювати копіювання ліцензійного програмного забезпечення, інформаційних баз даних і передавати їх іншим особам;

10) використовувати комп'ютерну техніку й установлене програмне забезпечення в цілях, що можуть призвести до пошкодження або втрати дієздатності комп'ютерної техніки, операційної системи чи комп'ютерної мережі Суду;

11) використовувати паролі, які застосовуються для доступу до ресурсів Мережі (у тому числі до робочих облікових записів), для особистих цілей (для облікового запису особистого провайдера послуг Інтернет, особистої електронної пошти тощо), а також зберігати їх в загальнодоступному місці на будь-яких фізичних чи електронних носіях;

12) залишати без нагляду ввімкнену Робочу станцію або робочий мобільний пристрій (планшет тощо) з можливим доступом до них сторонніх осіб;

13) відправляти електронною поштою будь-яку інформацію з обмеженим доступом;

14) вчиняти протиправні дії в мережі Суду або в інших мережах поза межами Суду, спрямовані на здійснення будь-яких видів атак на ресурси Мережі, а також порушення нормальної роботи мережевих служб і мережевого устаткування (несанкціонований доступ, підбір паролів, участь у DDoS-атаках тощо);

15) самостійно або за допомогою інших осіб підключати комп'ютерну техніку користувачів до Мережі в будь-який спосіб, що відрізняється від визначеного цим Положенням;

16) користуватися ресурсами мережі Інтернет у спосіб, що ускладнює надання послуг Інтернету та роботу Мережі, становить загрозу інформаційній безпеці Суду;

17) використовувати зовнішні носії інформації (диски, флеш-пам'ять тощо) без їх перевірки на предмет наявності шкідливого програмного забезпечення;

18) здійснювати будь-які види атак на ресурси Мережі, а також порушувати нормальну роботу мережевих служб і мережевого устаткування.

4. Усі користувачі комп'ютерної техніки Суду зобов'язані дотримуватися вимог цього Положення.

5. У разі виявлення порушень вимог Положення працівники управління інформаційних технологій та захисту інформації складають відповідний акт, який передають керівнику апарату Суду для вжиття необхідних заходів та повідомляють безпосереднього керівника Користувача (у разі наявності).

V. Підключення Користувача до Мережі

1. Питання оснащення робочого місця Користувача комп'ютерною технікою та її підключення до Мережі визначаються керівництвом Суду, виходячи з посадових обов'язків Користувача.

2. Користувач повинен володіти базовими знаннями та навичками роботи з комп'ютерною технікою та програмним забезпеченням, що використовуються ним у роботі.

3. Дозвіл на забезпечення робочого місця Користувача комп'ютерною технікою та її підключення до Мережі надається Адміністратором після подання службової записки за формою, наведеною у додатку 1 до цього Положення.

4. У разі зміни посади чи посадових обов'язків Користувача та необхідності зміни відповідних прав доступу до сервісів та служб, відповідні налаштування здійснюються Адміністратором після подання службової записки за формою, наведеною у додатку 3 до цього Положення.

5. У разі оперативної необхідності в наданні доступу до судових матеріалів, документів в комп'ютерній програмі «Д-3» та доступу до аудіо та відеоматеріалів у підсистемі Відеоконференцзв'язок (ВКЗ) для працівника управління забезпечення судового процесу, керівником цього управління чи особою, яка виконує його обов'язки, направляється лист на електронну пошту керівника управління інформаційних технологій та захисту інформації чи особи, яка виконує його обов'язки, з проханням надати відповідний доступ.

6. Самостійне підключення до Мережі суворо заборонене.

7. Встановлення комп'ютерної техніки на робочому місці Користувача, а також її підключення до Мережі здійснює безпосередньо Адміністратор лише після ознайомлення Користувача зі змістом цього Положення. Встановлення додаткових внутрішніх або зовнішніх пристроїв до комп'ютера Користувача здійснює виключно Адміністратор.

8. Комп'ютер встановлюється у місці, де обладнанню забезпечується нормальне охолодження. Повітря з вентилятора охолодження комп'ютера повинно мати вільний вихід.

VI. Відключення Користувача від Мережі

1. Користувач може бути відключений від Мережі у зв'язку з порушенням вимог цього Положення.

2. У разі звільнення Користувача, після підписання обхідного листа керівником управління інформаційних технологій та захисту інформації або особою, яка виконує його

обов'язки, Адміністратор відключає Користувача від Мережі (припиняє доступ до мережевих ресурсів та видаляє його облікові дані).

VII. Робота Користувача з комп'ютером у Мережі

1. На початку робочого дня Користувачу необхідно увімкнути Робочу станцію та здійснити вхід у Мережу.

2. У разі короткої перерви в роботі необхідно зберегти всі змінені впродовж останнього часу документи та ОБОВ'ЯЗКОВО зробити блокування комп'ютера, натиснувши комбінацію клавіш "CTRL" + "ALT" + "DEL" та натиснути на текстову кнопку «БЛОКУВАННЯ» або скористатись альтернативною комбінацією "Win" + "L".

3. Після завершення робочого дня Користувачу необхідно вимкнути комп'ютер. Перед вимкненням комп'ютера або його перезавантаженням необхідно закінчити роботу всіх програм.

4. У випадку некоректної роботи комп'ютера необхідно закінчити роботу всіх програм та перезавантажити комп'ютер.

5. У разі незвичайної роботи комп'ютера необхідно негайно повідомити про це Адміністратора.

6. Забороняється ставити на комп'ютерну техніку будь-які сторонні предмети, а також розміщувати поблизу комп'ютерної техніки речі й обладнання, що можуть негативно вплинути на її роботу.

7. Необхідно утримувати комп'ютерну техніку в чистоті, не допускати накопичення пилу на її поверхні, оберігати комп'ютерну техніку від різких струсів та вологості.

8. У разі технічної необхідності за вимогою Адміністратора Користувач зобов'язаний перезавантажити комп'ютер протягом 60 хв. У разі невиконання вимоги, Адміністратор має право самостійно перезавантажити такий робочий комп'ютер з попереднім повідомленням про це Користувача.

VIII. Доступ і використання даних у Мережі

1. Аутентифікація користувачів Мережі.

1) Права доступу в Мережі розподіляються на основі облікових даних користувачів.

2) Користувачам видаються унікальні ідентифікатори для роботи на комп'ютерах для захисту інформації від неавторизованого використання або перегляду.

3) Користувачам видаються тимчасові паролі до облікового запису Користувача на Робочій станції з обов'язковою вимогою їх заміни для захисту інформації від неавторизованого використання або перегляду. Адміністратор має право періодично контролювати використання інформації користувачами Мережі.

4) Ідентифікатори користувачів і їхні паролі повинні бути унікальними для кожного користувача.

5) Паролі повинні складатися як мінімум з 8 символів. У числі символів пароля обов'язково повинні бути присутніми букви у верхньому і нижньому регістрах, цифри і спеціальні символи (@, #, $, &, *, % тощо). Користувачі повинні добросовісно виконувати встановлені цим Положенням вимоги щодо створення паролів і не допускати використання легко вгадуваних паролів.

6) Паролі повинні триматися в таємниці, тобто не мають повідомлятися іншим людям, вставлятися в текст програм, зберігатися на комп'ютері в файлах текстових програм, записуватися на папір, наклеюватися на комп'ютер, монітор тощо. Повторне використання паролів заборонено.

7) Паролі підлягають періодичній заміні.

8) Позапланова зміна особистого пароля або видалення облікового запису Користувача у разі припинення його повноважень повинні проводитися Адміністратором негайно після закінчення останнього сеансу роботи цього Користувача з системою.

9) У разі компрометації особистого паролю Користувач повинен негайно вжити заходів щодо його зміни та повідомити про цей факт Адміністратора.

10) Адміністратор зобов'язаний вести паперовий або електронний журнал операцій створення, блокування, видалення облікових записів користувачів.

2. Використання електронної пошти.

1) Офіційні електронні адреси призначені для внутрішнього листування у Суді, а також листування, пов'язаного з виконанням посадових обов'язків з іншими суб'єктами, в тому числі з іншими судами, державними органів і установ, а також офіційними представниками міжнародних організацій.

2) Використання робочої електронної пошти в особистих цілях заборонено.

3) У випадку виявлення підозрілої активності щодо використання робочої електронної пошти Користувача, Адміністратор має право перевірити такі поштові відправлення.

4) У разі видалення Користувача з Мережі та за наявності технічної можливості поштова адреса Користувача може бути переадресована. Після закінчення терміну переадресації поштова адреса вилучається з системи або переводиться на іншого Користувача (за погодженням із керівництвом Суду).

5) Адміністратор забезпечує контроль за нормальним функціонуванням електронної пошти; відповідає за економне використання часу доступу до вузла провайдера послуг електронної пошти; інформує керівника про роботу електронної пошти, проблеми, що виникають в роботі, та шляхи їх усунення.

6) Відправка листів електронною поштою здійснюється тільки після їх перевірки на наявність шкідливого програмного забезпечення. Забороняється відправка електронних листів, які містять шкідливе програмне забезпечення.

7) Поштова програма забезпечує збереження інформації про відправлені та отримані повідомлення.

8) При формуванні електронного листа в рядку «Кому» вказується одна або декілька електронних адрес. Якщо виникає необхідність надсилання листів з використанням сталого переліку адрес, для зручності Користувач може згрупувати ці адреси і вказувати ім'я групи як електронну адресу.

9) При формуванні електронного листа в рядку «Тема» вказується його зміст у стислому вигляді. Якщо кінцевий адресат не має власної електронної адреси, в електронному листі треба вказати, кому адресована передана інформація (якщо ця інформація відсутня в рядку "Тема"). Для зменшення вірогідності потрапляння електронного листа в спам, рядок "Тема" підлягає заповненню.

10) У випадку надсилання файлів у тексті листа зазначається стисла інформація про файли, що приєднуються. Усі додані файли рекомендовано направляти у форматі "ZIP-архіву" або "RAR-архіву".

11) Максимальний розмір повідомлення з прикріпленими файлами для прийому та відправки у межах внутрішнього поштового серверу не повинен перевищувати 20 МБ. Розмір листа з прикріпленими файлами, що відправляється на зовнішні поштові сервери, може залежати від налаштувань та обмежень сервера одержувача. При відправці листів із вкладенням на зовнішні поштові сервери, рекомендований розмір листа не повинен перевищувати 15 Мб.

12) Додавати до електронних листів виконувані файли (з розширенням .exe, .com, .bat тощо) забороняється.

13) Якщо під час відправки електронного листа вказаний режим "Підтвердження доставки", то після доставки листа до поштової скриньки в автоматичному режимі буде надіслано повідомлення про доставку листа сервером отримувача.

14) Якщо під час відправки електронного листа вказаний режим "Підтвердження прочитання", то після доставки листа до поштової скриньки та підтвердження адресатом в

ручному режимі про прочитання отриманого листа буде надіслано повідомлення про прочитання адресатом цього листа.

15) Користувач зобов'язаний перевіряти електронну поштову скриньку не менше 2 разів на день (на початку першої та другої половин робочого дня).

16) У разі отримання електронного листа, який містить шкідливе програмне забезпечення, Користувач повідомляє Адміністратора про наявність такого у листі і вилучає інфікований електронний лист із папки "Вхідні", після чого очищує папку "Вилучені".

17) Обробці не підлягають електронні листи, в яких відсутня зворотна електронна адреса, зворотна електронна адреса невідома та в тексті листа відсутній підпис, за яким можливо ідентифікувати відправника. Відкривати файли, що приєднані до таких електронних листів, суворо забороняється.

18) У разі неможливості прочитати зміст електронного листа в результаті збою під час передачі, необхідно надіслати відправнику відповідне повідомлення.

19) З метою недопущення несанкціонованого використання електронної адреси Користувача, він зобов'язаний забезпечити блокування доступу до засобів електронної пошти з використанням паролю доступу.

3. Використання комп'ютерних програм.

1) Вимоги до комп'ютерних програм, що використовуються в Суді, визначаються виходячи з необхідності забезпечення виконання покладених на ці програми завдань та з урахуванням технічних параметрів наявних комп'ютерів, навичок роботи Користувачів з такими програмами та можливих витрат у разі переходу на інші комп'ютерні програми аналогічного призначення.

2) Придбання комп'ютерних програм здійснюється з урахуванням службової потреби та виходячи з посадових обов'язків Користувача. За потреби придбаваються виключно ліцензійні примірники програм або встановлюються примірники програм вільного використання. Ці програми повинні бути забезпечені документацією, що підтверджує правомірність їх використання згідно з ліцензією, або належність до комп'ютерних програм вільного використання.

3) Встановлення додаткових комп'ютерних програм на комп'ютері Користувача проводиться виключно Адміністратором після подання Користувачем службової записки на адресу сервісу технічної підтримки – support@vaks.gov.ua. Адміністратор має право уточнити необхідність використання таких програм у Користувача та/або його безпосереднього керівника/керівництва Суду.

4) Користувач зобов'язаний надавати доступ Адміністратору для встановлення (переустановлення) комп'ютерних програм або проведення їх інвентаризації.

5) Усі робочі станції повинні мати антивірусні програми з можливістю перевірки файлів при завантаженні на комп'ютер на предмет наявності вірусів.

4. Робота з документами.

1) Користувач або його керівник (у разі наявності) самостійно визначають, чи є документ необхідним тільки Користувачеві або іншим співробітникам, а також ступінь його конфіденційності. Якщо документ надалі необхідний іншим Користувачам, він може бути поміщений в директорію для спільної роботи, яка визначається Адміністратором.

2) Користувач зобов'язаний перевіряти файли з документами, а також файли на змінних носіях інформації (магнітних дисках, телефонах, відеокамерах, накопичувачах різних типів, оптичних пристроях, тощо), які підключає до комп'ютера, на якому він працює на наявність шкідливого програмного забезпечення за допомогою антивірусних програмних засобів.

3) Обмін інформацією між робочими станціями в локальній мережі здійснюється тільки через директорію, яку визначає Адміністратор.

5. Збереження і резервне копіювання інформації.

1) Збереження інформації забезпечується безперебійною роботою Мережі, що включає проведення комплексу спеціальних заходів (процедури обслуговування серверів баз даних; схеми збереження і відновлення баз даних; процедури моніторингу працездатності технічних

і програмних засобів, що забезпечують роботу структурних підрозділів з серверами баз даних; порядок дії в критичних ситуаціях).

2) Алгоритм резервного копіювання документів визначає Адміністратор.

6. Захист від шкідливого програмного забезпечення.

1) Обов'язковому контролю на предмет наявності шкідливого програмного забезпечення підлягає будь-яка інформація, що надходить та передається телекомунікаційними каналами, а також інформація на знімних носіях.

2) У разі виявлення під час проведення перевірки на предмет наявності шкідливого програмного забезпечення в ручному або автоматичному режимі заражених шкідливим програмним забезпеченням файлів, користувачі мережі зобов'язані:

– припинити роботу;

– негайно поінформувати про факт виявлення заражених шкідливим програмним забезпеченням файлів Адміністратора, власника заражених файлів, а також інших користувачів, що використовують ці файли в роботі;

3) Адміністратор спільно з Користувачем проводить аналіз необхідності подальшого їх використання. Знищення заражених файлів здійснюється Адміністратором в ручному або автоматичному режимі.

4) Відповідальність за проведення заходів антивірусного контролю, передбачених підпунктом 2 пункту 4 та підпунктом 3 пункту 7 розділу 8 цього Положення, покладається на користувачів.

7. Доступ до мережі Інтернет.

1) Користувачі використовують програми для пошуку інформації в мережі Інтернет із дотриманням принципів добросовісності та відповідальності.

2) При роботі з ресурсами мережі Інтернет неприпустимо: розголошування службової інформації; розповсюдження матеріалів, що захищаються авторськими правами та які використовують який-небудь патент, торгову марку, комерційну таємницю, права власності або авторські і суміжні з ним права третьої сторони; публікування, завантаження і розповсюдження матеріалів, що містять шкідливе програмне забезпечення, файли або програми, призначені для порушення, знищення або обмеження функціональності будь-якого комп'ютерного або телекомунікаційного устаткування або програм, для здійснення несанкціонованого доступу, а також серійні номери до комерційних програмних продуктів і програми для їх генерації, логіни, паролі й інші засоби для діставання несанкціонованого доступу до платних ресурсів в мережі Інтернет, а також розміщувати посилання на вищезгадану інформацію.

3) При роботі з ресурсами мережі Інтернет Користувачеві забороняється: завантажувати файли без попередньої перевірки на наявність шкідливого програмного забезпечення антивірусними програмами.

4) Користувачам локальної мережі Суду на робочих комп'ютерах заблоковано доступ до шкідливих та руйнівних ресурсів, які містять шкідливе програмне забезпечення, програми для зламу інформаційних систем із метою виводу їх з ладу або отримання несанкціонованого доступу до скачування інформації, сканери мереж, TCP-портів, ресурсів розважального характеру, зокрема служб знайомств і ресурсів порнографічного змісту, веб-казино, сайтів, які містять онлайнові веб-ігри, сервісів обміну даними та мовними повідомленнями, P2P-мереж (Emule, Gnutella, Gnutella 2, Torrent тощо), IP-телефонії, TOR-систем обміну інформацією.

5) Користувачам локальної мережі Суду на робочих комп'ютерах може бути заблоковано доступ до окремих соціальних мереж, музичних, фото- та відеоархівів; чат-серверів; ресурсів, які підтримують послуги передачі миттєвих повідомлень, зокрема ICQ, IRC тощо.

8. Організація віддаленого доступу Користувачами до Мережі

1) Віддалений доступ Користувача до Мережі надається за дозволом керівника апарату Суду на підставі поданої керівником відповідного структурного підрозділу (або помічником судді/суддею) службової записки за формою, наведеною у додатку 2 до цього Положення.

2) Для захищеного доступу до внутрішніх ресурсів Суду, надання віддаленого доступу здійснюється через VPN-сервіс, який координує Адміністратор.

3) VPN-сервіс повинен забезпечувати захищену передачу даних, шляхом програмного шифрування.

4) Паролі Користувачів до VPN-сервісів повинні регулярно змінюватись Адміністратором.

IX. Контроль за дотриманням вимог Положення

1. Контроль за дотриманням вимог Положення здійснює Адміністратор шляхом щомісячних і поточних перевірок.

2. Адміністратор має право знайомитися з документами, журналами й іншими матеріалами, які пов'язані з питаннями, що перевіряються.

3. Під час перевірки має бути присутній керівник структурного підрозділу (або особа, що його заміщує) Користувача, стосовно якого здійснюється перевірка дотримання вимог Положення.

4. За результатами перевірки складається акт, в якому зазначаються виявлені недоліки та пропозиції щодо їх усунення.

X. Відповідальність при роботі в Мережі

1. Користувач несе персональну відповідальність за дотримання встановлених вимог під час роботи в Мережі.

2. Відповідальність за допуск Користувача до Мережі і встановлення йому повноважень несе Адміністратор у межах вимог цього Положення.

3. Користувач, винний у порушенні законодавства України про захист прав власності і відомостей, що охороняються згідно із законом, несе відповідальність відповідно до чинного законодавства України.

Начальник управління
інформаційних технологій
та захисту інформації **Олександр ГРАЇЦЬКИЙ**

Додаток 1
До Положення
про порядок використання ресурсів
локальної комп'ютерної мережі у
Вищому антикорупційному суді

Адміністратору локальної
комп'ютерної мережі

СЛУЖБОВА ЗАПИСКА

Прошу забезпечити робоче місце Користувача:

☐ персональним комп'ютером;

☐ підключити автоматизоване робоче місце співробітника до локальної обчислюваної мережі, сервісів Вищого антикорупційного суду та глобальної мережі та надати відповідні права доступу;

☐ встановити/змінити додаткове програмне забезпечення на автоматизоване робоче місце співробітника та права доступу.

Відомості про Користувача		
Структурний підрозділ		
Користувач	посада	
	П. І. Б.	
Прізвище в латинській транскрипції		
Місцезнаходження (в тому числі кабінет)		
Контактний телефон	мобільний:	внутрішній:

Електронна пошта					
Підключити користувача до наступних список розсилок					
☒ всі	☐ держслужбовці	☐ патронатна служба	☐ секретарі	☐ керівники	☐ судді

Сервіси глобальних мереж	
Є доступ до інтернет ☐	Нема доступу до інтернет ☐

Офісне програмне забезпечення	
ПЗ для роботи з документами	☐
ПЗ для сканування та розпізнавання тексту	☐
ПЗ для роботи з електронною поштою	☐

Спеціалізоване ПЗ КП «Д-3»										
РНОКПП користувача										

Робота з документами				
Всі ☐	Всі по справах ☐	По справі судді _____ ☐	Поза справами ☐	Організаційно-розпорядчі ☐

Робота з прикріпленими файлами				
Всі ☐	Всі по справах ☐	По справі судді _____ ☐	Поза справами ☐	Організаційно-розпорядчі ☐

Робота зі справами				
Всі ☐	Всі по справах ☐	По справі судді _____ ☐		
Додаткова інформація:				

Інше спеціалізоване ПЗ та сервіси		
Система ISpro	☐	
M.E.Doc Station	☐	
SRS Femida (view)	☐	
Сервіс ВКЗ (vkz.court.gov.ua)	☐	
Віддалений доступ до записів судових засідань	☐	Суддя -

Додаткове ПЗ		
Антивірус та фаєрвол	☒	
Архіватор	☐	
Робота із зображеннями	Перегляд зображенньо ☐	Корегування растрових зображень ☐
Робота з відео	OBS Studio ☐	VLC media player ☐

Підключення до сервісів		
АРМ підключити до	Принтеру ☐	Багато-функціонального пристрою ☐

Мережеві папки		
Папка загального обміну	☐ Перегляд	☒ Редагування
	☐ Перегляд	☐ Редагування
	☐ Перегляд	☐ Редагування
	☐ Перегляд	☐ Редагування

Додаткові вимоги

_____ _____ _____ _____

(дата) (посада) (підпис) (ПІБ)

_____ _____ _____ _____

(дата) (посада) (підпис) (ПІБ)

Погоджено

Керівник апарату _____ **Богдан КРИКЛИВЕНКО**

(підпис)

Відмітка про виконання робіт		
Дата	Що зроблено	ПІБ виконавця, Підпис

Додаток 2
До Положення
про порядок використання ресурсів
локальної комп'ютерної мережі у
Вищому антикорупційному суді

Керівникові апарату
Вищого антикорупційного суду
Богдану КРИКЛИВЕНКУ

Службова записка

Прошу надати мені доступ до свого робочого комп'ютеру для дистанційної роботи.

Доступ потрібен на період з ☐☐:☐☐:☐☐☐☐ по ☐☐:☐☐:☐☐☐☐

Підтверджую про ознайомлення з ймовірними ризиками та потенційними загрозами безпеці при роботі через віддалений режим.

Дата **Підпис**

Начальник управління інформаційних
технологій та захисту інформації **Олександр ГРАЇЦЬКИЙ**

Додаток 3
До Положення
про порядок використання ресурсів
локальної комп'ютерної мережі у
Вищому антикорупційному суді

Адміністратору локальної
комп'ютерної мережі

СЛУЖБОВА ЗАПИСКА

Прошу внести зміни у конфігурацію робочого місця Користувача:

Відомості про користувача												
Структурний підрозділ												
Користувач	посада											
	П. І. Б.											
Прізвище в латинській транскрипції												
Місцезнаходження (в тому числі кабінет)												
Контактний телефон	мобільний:								внутрішній:			

Електронна пошта					
Підключити користувача до наступних список розсилок					
☒ всі	☐ держслужбовці	☐ патронатна служба	☐ секретарі	☐ керівники	☐ судді

Спеціалізоване ПЗ КП «Д-3»				
Робота з документами				
Всі ☐	Всі по справах ☐	По справі судді _____ ☐	Поза справами ☐	Організаційно-розпорядчі ☐
Робота з прикріпленими файлами				
Всі ☐	Всі по справах ☐	По справі судді _____ ☐	Поза справами ☐	Організаційно-розпорядчі ☐
Робота зі справами				
Всі ☐	Всі по справах ☐	По справі судді _____ ☐		
Додаткова інформація:				

Інше спеціалізоване ПЗ та сервіси		
Система ISpro		☐
M.E.Doc Station		☐
SRS Femida (view)		☐
Сервіс ВКЗ (vkz.court.gov.ua)		☐
Віддалений доступ до записів судових засідань	☐	Суддя -

Мережеві папки		
Папка загального обміну	☐ Перегляд	☒ Редагування
	☐ Перегляд	☐ Редагування
	☐ Перегляд	☐ Редагування

	☐ Перегляд	☐ Редагування

Додаткові вимоги

_____ _____ _____ _____

(дата) (посада) (підпис) (ПІБ)

_____ _____ _____ _____

(дата) (посада) (підпис) (ПІБ)

Погоджено

Керівник апарату _____ **Богдан КРИКЛИВЕНКО**

(підпис)

Відмітка про виконання робіт		
Дата	Що зроблено	ПІБ виконавця, Підпис