ДЕСНЯНСЬКА РАЙОННА В МІСТІ КИЄВІ ДЕРЖАВНА АДМІНІСТРАЦІЯ

РОЗПОРЯДЖЕННЯ

24.06.2022 № 210

Про затвердження Порядку використання ресурсів локальної комп'ютерної мережі в Деснянській районній в місті Києві державній адміністрації

Відповідно до законів України «Про місцеві державні адміністрації», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», Указу Президента України від 14 вересня 2020 року № 392/2020 «Про рішення Ради національної безпеки і оборони України від 04 вересня 2020 року «Про Стратегію національної безпеки України», постанов Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», від 12 березня 2022 року № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» та з метою забезпечення правильного та ефективного використання в роботі комп'ютерного устаткування, ресурсів мережі Інтернет, електронної пошти, забезпечення кібербезпеки в процесі цифрової трансформації, а також умов зберігання інформації та її розповсюдження в Деснянській районній в місті Києві державній адміністрації:

1. Затвердити Порядок використання ресурсів локальної комп'ютерної мережі в Деснянській районній в місті Києві державній адміністрації, що додається.

2. Визначити Адміністратором, що здійснює адміністрування

серверів і робочих станцій, а також проєктування і розвиток локальної комп'ютерної мережі в Деснянській районній в місті Києві державній адміністрації відділ інформаційних технологій Деснянської районної в місті Києві державної адміністрації.

3. Під час дії воєнного стану користувачам локальної комп'ютерної мережі Деснянської районної в місті Києві державної адміністрації в своїй роботі користуватись Інструкцією з кібергігієни та кібербезпеки Деснянської районної в місті Києві державної адміністрації.

4. Визнати таким, що втратило чинність розпорядження Деснянської районної в місті Києві державної адміністрації від 04 листопада 2016 року № 649 «Про затвердження Положення про порядок використання ресурсів локальної комп'ютерної мережі в Деснянській районній в місті Києві державній адміністрації».

5. Контроль за виконанням цього розпорядження покласти на керівника апарату Деснянської районної в місті Києві державної адміністрації О. Машківську.

Голова Дмитро РАТНІКОВ

ЗАТВЕРДЖЕНО

Розпорядження Деснянської районної в місті Києві державної адміністрації
від 24 червня 2022 № 210

ПОРЯДОК
використання ресурсів локальної комп'ютерної мережі в Деснянській районній в місті Києві державній адміністрації

Порядок використання ресурсів локальної комп'ютерної мережі в Деснянській районній в місті Києві державній адміністрації визначає механізм підключення до локальної комп'ютерної мережі, доступу до інформаційних ресурсів, які містять необхідні вимоги щодо забезпечення спільної роботи в локальній комп'ютерній мережі, збереження інформації користувачів мережі і дотримання прав на її розповсюдження.

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

1. Основні терміни

1.1. Мережа - локальна комп'ютерна мережа, розміщена в приміщенні Деснянської районної в місті Києві державної адміністрації (далі - Деснянська райдержадміністрація), сукупність комп'ютерів, серверів, кабельна система, сукупність мережевих адаптерів, активного мережевого обладнання, що працює під управлінням мережевих операційних систем і прикладного програмного забезпечення, до якої підключені працівники Деснянської райдержадміністрації.

1.2. Адміністратор - відділ інформаційних технологій Деснянської райдержадміністрації, що здійснює адміністрування серверів і робочих станцій, а також проєктування і розвиток Мережі.

1.3. Користувач - працівник Деснянської райдержадміністрації, персональний комп'ютер якого має підключення до Мережі.

2. Загальні умови користування Мережею

2.1. З метою забезпечення стабільного функціонування Мережі Користувач зобов'язаний дотримуватися вимог цього Положення, а також неухильно дотримуватись рекомендацій Адміністратора.

2.2. При користуванні Мережею забороняється:

2.2.1. Здійснювати пошкодження, знищення або фальсифікацію сторонньої інформації;

2.2.2. Здійснювати будь-які види атак на ресурси Мережі, а також порушувати нормальну роботу мережевих служб і мережевого устаткування;

2.2.3. Розповсюджувати інформацію, заборонену чинним законодавством України або яка не відповідає морально-етичним нормам її одержувачів, а також розсилати недостовірні або загрозливі повідомлення;

2.2.4. Здійснювати масову розсилку електронних повідомлень, у тому числі «спаму»;

2.2.5. Використовувати обмежені ресурси Мережі без дозволу Адміністратора;

2.2.6. Використовувати надані ресурси не за призначенням.

2.3. Порушення вимог цього Положення може бути підставою до припинення доступу Користувача до Мережі. Відключення може бути тимчасовим, умовно безстроковим (відновлюється при клопотанні керівника Користувача), безстроковим.

2.4. Управління Мережею здійснює Адміністратор, шляхом виконання робіт щодо супроводу і розвитку Мережі, підключення до Мережі, припинення доступу до Мережі, здійснення контролю за використанням ресурсів Мережі її Користувачами.

2.5. Інформація про ресурси та функціонування локальної комп'ютерної Мережі або окремих її елементів становить службову інформацію.

3. Відповідальність, права і обов'язки Адміністратора

3.1. Адміністратор несе відповідальність за:

3.1.1. Функціонування Мережі в цілому;

3.1.2. Функціонування сервісів Мережі;

3.2. Порушення функціонування Мережі у зв'язку з некоректним управлінням маршрутизацією та базовими мережевими сервісами.

3.3. Адміністратор зобов'язаний:

3.3.1. Обмежити доступ співробітників і сторонніх відвідувачів у приміщення, в яких встановлені сервери і комутаційне устаткування Мережі;

3.3.2. Забезпечити контроль структури Мережі;

3.3.3. Здійснювати організаційні (контроль за дотриманням правил користування комп'ютерною технікою) та технічні (регулярна заміна мережевих паролів, відстеження запуску і припинення використання програмного забезпечення, що порушує нормальну працездатність Мережі, комп'ютерів в ній і безпеку Мережі) заходи щодо припинення несанкціонованого підключення до Мережі із зовнішніх мереж, а також із комп'ютерів Мережі;

3.3.4. Здійснювати керівництво роботами, пов'язаними з впровадженням нових технологій і розвитком Мережі;

3.3.5. Проводити заходи щодо забезпечення безпеки в Мережі;

3.3.6. Подавати пропозиції про необхідність придбання нових ліцензійних комп'ютерних програм, забезпечувати отримання необхідних комп'ютерних програм, що розповсюджуються на безоплатній основі;

3.3.7. Надавати Користувачам консультаційну допомогу з питань використання ресурсів Мережі.

3.4. Адміністратор має право:

3.4.1. Відключати Мережу, якщо зафіксовано вірусну активність, до усунення останньої;

3.4.2. Відключати Мережу, якщо заздалегідь відомо про відключення електроживлення;

3.4.3. Частково або повністю припинити доступу Користувача до Мережі відповідно до пункту 2.3 розділу 2 та розділу 6 цього Положення.

3.4.4. Приймати рішення щодо адміністративних питань взаємодії з користувачами Мережі.

4. Права і обов'язки Користувача

4.1. Користувач має право:

4.1.1. На доступ до ресурсів Мережі відповідно до вимог цього Положення та посадових обов'язків;

4.1.2. Надавати Адміністратору зауваження та пропозиції щодо роботи Мережі;

4.1.3. Звертатися за довідковою інформацією і консультацією до Адміністратора.

4.2. Користувач зобов'язаний:

4.2.1. Використовувати всі ресурси Мережі тільки в робочих цілях;

4.2.2. Виконувати вимоги Адміністратора згідно з цим Положенням;

4.2.3. Дотримуватися правил техніки безпеки при роботі з технічними засобами;

4.2.4. Забезпечити нерозголошення ідентифікаційної інформації, яка використовується для доступу до ресурсів Мережі;

4.2.5. Перешкоджати несанкціонованому і недобросовісному використанню ресурсів Мережі;

4.2.6. Використовувати антивірусні програми, встановлені Адміністратором;

4.2.7. Дотримуватися законодавства з питань правової охорони комп'ютерних програм та виконувати умови їх використання.

4.3 Користувачі несуть персональну відповідальність при роботі з паролями, дотриманням порядку їх зміни, зберігання і використання.

5. Підключення Користувача до Мережі

5.1. Необхідність оснащення робочого місця Користувача комп'ютером та його підключення до Мережі визначається керівником Користувача.

5.2. Користувач повинен володіти базовими знаннями та навичками роботи на комп'ютері та з програмним забезпеченням, що буде встановлено на його робочому місці.

5.3. Дозвіл на підключення комп'ютера Користувача до Мережі надається Адміністратором. Самостійне підключення є грубим порушенням цього Положення.

5.4. Встановлення комп'ютера та периферійних пристроїв на робочому місці Користувача здійснює безпосередньо Адміністратор лише після ознайомлення Користувача зі змістом цього Положення. Встановлення додаткових внутрішніх або зовнішніх пристроїв до комп'ютера Користувача здійснює виключно Адміністратор.

5.5. Комп'ютер встановлюється у місці, де забезпечується необхідне охолодження обладнання. Повітря з вентилятора охолодження комп'ютера повинно мати вільний вихід.

6. Припинення доступу Користувача до Мережі

6.1. Користувачеві може бути припинено доступ до Мережі у зв'язку з порушенням вимог цього Положення.

6.2. Рішення про припинення доступу Користувача до Мережі приймається Адміністратором.

6.3. У разі припинення трудових відносин з Користувачем та підписання обхідного листа Адміністратор відключає Користувача від Мережі (припиняє доступ до мережних ресурсів та видаляє його ідентифікаційні данні).

7. Робота Користувача з комп'ютером у Мережі

7.1. На початку робочого дня необхідно ввімкнути комп'ютер та здійснити реєстрацію в локальній мережі.

7.2. У разі короткої перерви в роботі необхідно зберегти всі змінені впродовж робочого періоду документи та зробити блокування комп'ютера, натиснувши комбінацію клавіш «CTRL» + «ALT» + «DEL» або «Win» + «L».

7.3. Перед закінченням роботи з комп'ютером у кінці робочого дня або у разі залишення робочого місця завчасно до кінця робочого дня необхідно вимкнути комп'ютер.

7.4. Перед вимкненням комп'ютера або його перезавантаженням необхідно закінчити роботу всіх програм.

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

7.6. У разі, якщо Користувачем зафіксовано виконання персональним комп'ютером задач/завдань (команд), що користувачем не надавались, необхідно негайно повідомити про це Адміністратора.

7.7. Забороняється пересувати ввімкнений комп'ютер.

7.8. Забороняється самостійно, без дозволу Адміністратора, здійснювати встановлення комп'ютеру в інше місце/кабінет.

7.9. Забороняється ставити на системний блок будь-які сторонні предмети.

7.10. Забороняється встановлювати комп'ютер у місцях, де існує небезпека потрапляння на нього води, а також поблизу опалювальних приладів.

7.11. Необхідно утримувати комп'ютер в чистоті, не допускати накопичення пилу на поверхні, оберігати комп'ютер від різких струсів та вологості.

8. Доступ і використання даних у Мережі

8.1. Аутентифікація користувачів Мережі:

8.1.1. Права доступу в Мережі розподіляються на основі облікових даних Користувачів.

8.1.2. Користувачам видаються ідентифікатори і паролі для роботи на комп'ютерах для захисту інформації від неавторизованого використання або перегляду. Ці паролі не захищають від перегляду інформації Адміністратором, який має право періодично контролювати використання інформації користувачами Мережі.

8.1.3. Ідентифікатори Користувачів і їх паролі повинні бути унікальними для кожного Користувача.

8.1.4. 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). Легко вгадуванні паролі Користувачі повинні негайно змінити.

8.1.5. Заборонено передавати особисті паролі стороннім особам, іншим Користувачам, фіксувати їх на номерах чи інших носіях.

8.1.6. Позапланова зміна особистого пароля або видалення облікового запису Користувача у разі припинення його повноважень проводяться Адміністратором негайно після закінчення останнього сеансу роботи даного Користувача з системою.

8.1.7. У разі компрометації особистого паролю Користувача необхідно негайно вжити заходів щодо його зміни Адміністратором залежно від повноважень власника скомпрометованого паролю.

8.1.8. Питання тимчасового блокування та розблокування облікового запису або заміни часу доступу до нього вирішується Адміністратором.

8.2. Використання електронної пошти:

8.2.1. Офіційні електронні адреси призначені для здійснення службового листування працівниками Деснянської райдержадміністрації, офіційними представниками інших органів і установ, а також офіційними представниками міжнародних організацій. Використання електронних адрес для неофіційного листування забороняється.

8.2.2. Перелік офіційних електронних адрес для здійснення службового листування створюється Адміністратором.

8.2.3. Адміністратор має право здійснювати спостереження за поштовими відправленнями користувачів Мережі.

8.2.4. У разі видалення Користувача з Мережі за погодженням Адміністратора поштова адреса Користувача блокується.

8.2.5. Адміністратор забезпечує контроль за: правильним функціонуванням електронної пошти; відповідає за економне використання часу доступу до вузла провайдера послуг електронної пошти; інформує керівника апарату Деснянської райдержадміністрації про роботу електронної пошти, проблеми, що виникають при її функціонуванні, та шляхи їх усунення.

8.2.6. Відправка листів електронною поштою здійснюється тільки після їх перевірки на наявність комп'ютерних вірусів. Забороняється відправка електронних листів, які містять комп'ютерні віруси.

8.2.7. Поштова програма забезпечує збереження інформації про відправлені та отримані повідомлення.

8.2.8. Відправка офіційних листів електронною поштою здійснюється тільки після реєстрації документів на паперових носіях та запису вихідного реєстраційного номера і дати документа в комп'ютерному файлі відповідного документа. Офіційні документи, що вкладаються до електронного листа-повідомлення, за умови впровадження електронного цифрового підпису, обов'язково підписуються з використанням посиленого сертифікату відкритого ключа після внесення реєстраційних дати та номера, особою що реєструє та відправляє лист.

8.2.9. Офіційні електронні адресні складаються з префікса "name@" та відповідного доменного імені kmda.gov.ua

8.2.10. Відправка електронних листів здійснюється тільки з електронних адрес, занесених до реєстру електронних адрес Адміністратором.

8.2.11. Забороняється здійснювати масову розсилку (розсилка безлічі одержувачів, або множинна розсилка одному одержувачу) не узгоджених заздалегідь електронних листів, а також розсилку електронних листів рекламного, комерційного або агітаційного характеру та листів, що містять грубі і образливі вирази і пропозиції.

8.2.12. При формуванні електронного листа в рядку «Кому» вказується одна або декілька електронних адрес.

8.2.13. 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»). Рядок «Тема» заповнюється обов'язково.

8.2.14. У випадку приєднання файлів у листі необхідно давати стислу інформацію про файли, що приєднуються.

8.2.15. Сумарний об'єм файлів, що приєднуються до електронного повідомлення, не повинен перевищувати 15 Мегабайт (Мб). У разі, коли розмір файлу перевищує 15 Мб, необхідно зробити багатотомний архів з розбиттям на частини до 15 Мб та надіслати кожну частину окремим електронним листом. У кожному листі в рядку «Тема» в кінці найменування листа в дужках вказується поточний номер частини листа та через символ «/» загальна кількість листів.

8.2.16. Додавати до електронних листів файли, що виконуються (EXE, COM, BAT тощо), без їх архівації забороняється.

8.2.17. Кожний офіційний електронний лист має бути підписаний. Підпис складається з наступних рядків:

посада Користувача та назва підрозділу;
прізвище, ім'я, по батькові відправника;
код міжміського зв'язку (оператора мобільного зв'язку) та телефон;
e-mail адреса.

8.2.18. Якщо під час відправки електронного листа вказаний режим «Підтвердження отримання», то після доставки листа до поштової скриньки в автоматичному режимі буде надіслано повідомлення про отримання адресатом цього листа.

8.2.19. 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.

8.2.20. Після відправки електронних листів з офіційних електронних адрес, перелік яких створено відповідно до п. 8.2.2. цього Положення, Користувач:

підшиває в номенклатурну справу з відправленими документами,

документ та додатки до нього, на підставі яких було сформовано офіційний електронний лист;

здійснює контроль надходження підтверджень від адресатів про отримання електронних листів (у разі необхідності);

друкує, підписує та підшиває в окрему справу реєстр вхідної та вихідної інформації.

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

8.2.22. Після отримання нових повідомлень електронною поштою Користувач:

перевіряє на повноту та відповідність реєстраційних реквізитів, вказаних в темі і приєднаних файлах, а також коректність змісту приєднаних файлів;

у разі отримання електронного листа, який містить комп'ютерні віруси, надсилає відправнику повідомлення про наявність у листі комп'ютерних вірусів та необхідність відправки нового листа і вилучає інфікований електронний лист із папки «Вхідні», після чого очищує папку «Вилучені»;

надсилає електронною поштою підтвердження про отримання повідомлення відправнику (якщо про це є повідомлення в листі) або повідомлення про проблеми з читанням отриманого листа.

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

8.2.24. У разі неможливості прочитати зміст електронного листа в результаті збою при передачі, необхідно надіслати відповідне повідомлення відправнику.

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

8.3. Використання комп'ютерних програм:

8.3.1. Вимоги до комп'ютерних програм, що використовуються в Деснянській райдержадміністрації визначаються, виходячи з необхідності забезпечення виконання покладених на них 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.

8.3.2. Придбання комп'ютерних програм здійснюється з урахуванням потреби. При цьому придбаваються виключно ліцензійні примірники таких програм або примірники програм вільного використання, які повинні бути забезпечені документацією, що підтверджує правомірність їх використання згідно з ліцензією або належність до комп'ютерних програм вільного

використання.

8.3.3. Встановлення додаткових комп'ютерних програм на комп'ютері Користувача проводиться виключно Адміністратором. Забороняється проводити інсталяцію додаткових програм без відома Адміністратора.

8.3.4. Користувач зобов'язаний надавати доступ Адміністратору для встановлення (переустановлений) комп'ютерних програм та перевірки встановленого програмного забезпечення.

8.3.5. Усі робочі станції повинні мати резидентні антивірусні програми з можливістю перевірки на віруси файлів при завантаженні на комп'ютер.

8.4. Робота з документами:

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

8.4.2. Файли з документами необхідно зберігати тільки в директорії, яку визначає Адміністратор (з метою коректної роботи режиму резервного копіювання документів з поточного комп'ютера на сервер), у разі наявності такої можливості.

8.4.3. Перед копіюванням або відкриттям будь-якого файлу, який відсутній на жорсткому диску комп'ютера, його необхідно перевірити на наявність вірусів за допомогою антивірусної програми.

8.4.4. Забороняється працювати в режимі корегування документів, які знаходяться не на жорсткому диску комп'ютера.

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

8.5. Збереження і резервне копіювання інформації:

8.5.1. 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).

8.5.2. Алгоритм резервного копіювання документів визначає Адміністратор.

8.6. Антивірусний захист:

8.6.1. Обов'язковому антивірусному контролю підлягає будь-яка інформація, що надходить та передається по комунікаційних каналах, а також інформація на знімних носіях.

8.6.2. У разі виявлення при проведенні антивірусної перевірки заражених комп'ютерними вірусами файлів Користувачі мережі зобов'язані:

припинити роботу;

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

спільно з власником заражених вірусом файлів провести аналіз необхідності подальшого їх використання;

провести лікування або знищення заражених файлів;

у разі виявлення нового вірусу який не піддається лікуванню антивірусними засобами, знищити його;

8.6.3. Відповідальність за проведення заходів антивірусного контролю на комп'ютерах і дотримання вимог цього Порядку покладається на Користувачів.

8.7. Доступ до мережі Інтернет:

8.7.1. Користувачі використовують програми для пошуку інформації в мережі Інтернет тільки для виконання ними своїх посадових обов'язків.

8.7.2. При роботі з ресурсами мережі Інтернет неприпустимо: розголошування службової інформації; розповсюдження матеріалів, що захищаються авторськими правами, та які використовують патент, торгову марку, комерційну таємницю, права власності або авторські і суміжні з ним права третьої сторони; публікування, завантаження і розповсюдження матеріалів, що містять віруси, файли або програми, призначені для порушення, знищення або обмеження функціональності будь-якого комп'ютерного або комунікаційного 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 Інтернеті, а також розміщувати посилання на вищезгадану інформацію.

8.7.3. При роботі з ресурсами Інтернет Користувачеві забороняється: завантажувати файли без попередньої перевірки на наявність вірусів встановленим антивірусним пакетом.

8.7.4. Дії Користувача, якими порушено правила користування мережею Інтернет, можуть бути запротокольовані, і використовуватися для ухвалення рішення про застосування до нього заходів дисциплінарного впливу.

9. Обслуговування локальної комп'ютерної мережі

9.1. Проведення робіт з модернізації, ремонту та відновленню роботи локальної комп'ютерної мережі здійснює Адміністратор. Адміністратор, у разі необхідності та за погодженням із керівником апарату Деснянської районної в місті Києві державної адміністрації, може долучати до проведення робіт передбачених цим пунктом сторонніх спеціалістів з відповідними кваліфікаційними знаннями та досвідом роботи.

9.2. Для виконання робіт передбачених пунктом 9.1 цього Положення, Адміністратору надається безперешкодний доступ в приміщення, де розміщено окремі елементи локальної комп'ютерної мережі.

9.3. У разі проведення планових робіт пов'язаних із відключенням доступу Користувачів до локальної комп'ютерної мережі та мережі Інтернет Адміністратор зобов'язаний поінформувати відповідні структурні підрозділи про проведення таких робіт не пізніше ніж за два дні до початку їх проведення.

9.4. Строк виконання робіт передбачених пунктом 9.1. цього Положення визначається Адміністратором та залежить від складності їх виконання, часу необхідного для проведення налаштування та тестування обладнання.

10. Контроль за виконанням правил доступу до Мережі

10.1. Контроль за виконанням правил доступу і використання локальної комп'ютерної мережі здійснює Адміністратор шляхом проведення планових і позапланових перевірок.

10.2. Адміністратор має право знайомитися з документами, журналами та іншими матеріалам, що мають відношення до питань, які перевіряються.

10.3. Під час перевірки має бути присутній керівник структурного підрозділу, що перевіряється, або особа, що його заміщує.

10.4. За результатами перевірки складається акт з виявленими недоліками і пропозиції щодо їх усунення.

11. Відповідальність при роботі в Мережі

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

11.2. Відповідальність за допуск Користувача до Мережі і встановлення йому повноважень несе керівник структурного підрозділу та Адміністратор.

11.3. Користувачі, винні в порушенні законодавства України про захист прав власності і відомостей, що охороняються згідно із законом, несуть дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність відповідно до чинного законодавства України.

Керівник апарату Ольга МАШКІВСЬКА