З А Т В Е Р Д Ж Е Н О
Наказ керівника Київської
обласної прокуратури
«2» червня 2021 року № 92

Положення

про порядок користування комп'ютерною технікою та інформаційно-телекомунікаційними системами в Київській обласній прокуратурі

1. Загальні положення

1.1. Правила користування комп'ютерною технікою та інформаційно-телекомунікаційними системами (далі - Правила) створені з метою регламентування роботи користувачів персональних комп'ютерів, забезпечення інформаційної безпеки при роботі в різних інформаційних системах та ефективного використання інформаційних ресурсів, що функціонують у Київській обласній прокуратурі.

1.2. Інформаційні та інформаційно-телекомунікаційні системи, у яких циркулює інформація з обмеженим доступом (секретна та інформація, що містить службову інформацію з грифом обмеження доступу «Для службового користування»), використовуються відповідно до вимог нормативно-правових актів у сфері охорони інформації з обмеженим доступом.

2. Терміни та скорочення

Персональний комп'ютер (ПК) - електронна обчислювальна машина, яка складається з системного блоку, монітору, клавіатури та маніпулятора «миша», а також необхідних з'єднувальних кабелів для підключення до електро та локальної мережі, телекомунікаційного обладнання. Конфігурація може відрізнятися залежно від виробника. Також у Правилах під поняттям «ПК» слід розуміти ноутбуки, моноблоки, планшетні комп'ютери.

Інформаційна система (ІС), інформаційно-аналітична система (ІАС) - сукупність організаційних і технічних засобів для збирання, пошуку, обробки, аналізу, збереження, пересилання інформації з метою забезпечення інформаційних потреб користувачів (ІАС «ОСОП», ІС «СЕД»).

Телекомунікаційна система (ТС) - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Програмно-апаратний комплекс - це набір технічних та програмних

засобів, що працюють спільно для виконання одного, або більше завдань.

Інформаційні ресурси - масиви зберігання інформації в інформаційних системах.

Периферійні пристрої - електронні засоби сканування, друку, передачі та накопичення інформації в комплекті з необхідним набором кабелів для підключення.

Операційна система (ОС) - базове програмне забезпечення, яке виконує управління апаратним забезпеченням ПК, керує обчислювальним процесом і організовує взаємодію з користувачем. Найбільш відомі ОС: MS Windows, MacOS, Linux, Android.

Апаратне забезпечення (АЗ) - комплекс технічних засобів ПК, його фізична частина.

Програмне забезпечення (ПЗ) - сукупність програм ПК, за допомогою яких виконується обробка інформації.

Відділ інформаційних технологій (ВІТ) - структурний підрозділ Київської обласної прокуратури, до компетенції якого віднесено впровадження і забезпечення роботи інформаційно-телекомунікаційних систем та програмно-апаратних комплексів.

Комп'ютерна техніка (КТ) - ПК та обладнання, що працює спільно з ПК (периферійні пристрої).

Спам - масова розсилка кореспонденції рекламного чи іншого характеру користувачам, які не висловили бажання її отримувати.

Локально-обчислювальна мережа (ЛОМ) - програмно-апаратний комплекс для об'єднання ПК в одне фізичне середовище.

Файловий сервер - сервер, призначений для зберігання і забезпечення спільного доступу користувачів до інформації (файлів).

Файловий інформаційний ресурс - сукупність файлів та папок, що зберігаються в каталозі локальної файлової системи (який називається корневим каталогом файлового інформаційного ресурсу), доступний користувачам, як персоналізовано так і анонімно.

Виділений інформаційний ресурс - сукупність файлів та папок, що зберігаються в каталозі локальної файлової системи (який називається корневим каталогом файлового інформаційного ресурсу), доступний користувачам, які об’єднані в одну робочу групу та наділені рівними правами відповідно до повноважень підрозділу.

Персональний інформаційний ресурс - сукупність файлів та папок, що зберігаються в каталозі локальної файлової системи (який називається корневим каталогом файлового інформаційного ресурсу), доступний певному користувачу

лише персоналізовано, створюється за його бажанням. Доступ інших осіб до вказаного ресурсу заблоковано.

ВКЗ – відеоконференцзв'язок.

3. Використання персонального комп'ютера

3.1. Персональний комп'ютер (ПК) повинен використовуватися тільки в службових цілях.

3.2. Під час завантаження ПК і авторизації в операційній системі (ОС) користувачу необхідно прослідкувати, чи не з'являються повідомлення про помилки ОС або програмного забезпечення (ПЗ). У разі виникнення таких помилок і неможливості усунути їх власноруч необхідно повідомити про це працівників ВІТ.

3.3. Після повного завантаження ОС та супутнього ПЗ потрібно переконатися, що антивірусний захист працює належним чином (є індикатор антивірусу і відсутні попереджувальні повідомлення про його обмежену чи невірну роботу).

3.4. Перевірити, чи не видає ПК сторонніх звуків, які б могли сигналізувати про несправність техніки. Якщо такі звуки присутні, необхідно повідомити про це працівників ВІТ.

3.5. Обслуговування комп'ютерної техніки (КТ) проводиться виключно спеціалістами ВІТ та працівниками структурних підрозділів, які наділені аналогічними повноваженнями згідно з Положеннями про самостійні підрозділи. У разі обслуговування КТ, на якій обробляється інформація з обмеженим доступом, воно здійснюється спеціалістами ВІТ та працівниками структурних підрозділів, які наділені аналогічними повноваженнями з відповідним допуском.

3.6. Під час переїздів співробітників до інших приміщень працівники ВІТ забезпечують лише відключення і підключення КТ.

3.7. При користуванні КТ забороняється:

- самостійне внесення зміни в конфігурацію ПК, розбирання ПК, принтерів та інших периферійних пристроїв;

- переміщення, у тому числі вивезення зі службових приміщень КТ, що перебуває на обліку в Київській обласній прокуратурі, без узгодження з ВІТ;

- встановлення ПЗ без узгодження з фахівцями ВІТ, особливо такого, яке може становити загрозу роботі ПК та ЛОМ (антивіруси, мережеві екрани, мережеві сканери тощо);

- видалення встановленого ПЗ або його зміна на інше, оскільки встановлення додаткових програм може викликати конфлікт з уже існуючими та вивести ПК з ладу;

- у разі відсутності користувача на робочому місці залишення ПК увімкнутим, або незаблокованим, що може зумовити можливість використання

ПК сторонніми особами;

- термічного, хімічного, фізичного впливу на ПК та периферійне обладнання.

3.8. Підключення до локально-обчислювальної мережі (ЛОМ) та зміна мережевих налаштувань здійснюється виключно спеціалістами ВІТ.

3.9. У разі припинення друку на ввіреній техніці периферійного пристрою та наявність повідомлення про закінчення тонеру на панелі принтеру, користувач повинен самостійно та обережно вилучити картридж з пристрою та передати до ВІТ. У разі наявності інших проблем під час друку (дублювання відтиску, чорніння тощо), роздруковується тестова сторінка друку, яка також доставляється разом з картриджем до ВІТ.

3.10. ПК та периферійні пристрої закріплюється персонально за певним користувачем.

3.11. Забороняється використовувати особисту комп'ютерну та телекомунікаційну техніку в локальній мережі Київської обласної прокуратури, без узгодження з працівниками ВІТ.

3.12. Кожен користувач повинен слідкувати за справністю ввіреної йому техніки, дбайливо до неї ставитися, тримати її в чистоті та належному стані.

3.13. У разі недбалого ставлення, що призвело до виходу техніки з ладу, несанкціонованого доступу до інформаційних систем, мереж, баз даних, втрати чи спотворення даних тощо з певного ПК, користувач несе персональну відповідальність відповідно до чинного законодавства.

3.14. Під час використання КТ, користувач має забезпечити зберігання інформації на робочому місці.

3.15. З приводу використання комп'ютерної техніки, мережевих ресурсів, засобів електронної пошти, мережі інтернет та інших питань, визначених цим положенням слід звертатися до спеціалістів ВІТ.

4. Використання і зберігання паролів

Простий (слабкий) пароль підвищує потенційний ризик несанкціонованого доступу до інформаційних систем та фактів компрометації облікових записів користувача.

4.1. Пароль є конфіденційною інформацією і не підлягає розголошенню.

4.2. Не рекомендується використовувати один і той самий пароль для доступу до різних ІС, ІАС тощо.

4.3. При використанні і зберіганні паролів слід уникати:

- можливості іншої особи працювати з власним обліковим записом;

- озвучення паролів;

- повідомлення своїх паролів телефоном, електронною поштою, через мережу Інтернет тощо;

- зазначення своїх паролів в анкетах (формах, бланках);

- записів паролів і відкрите їх зберігання на робочому місці;

- зберігання паролів у файлі на комп'ютері (планшеті, телефоні тощо) без забезпечення умов обмеження доступу сторонніх осіб;

- використання функції *«Запам'ятати пароль»,* що може пропонувати деяке програмне забезпечення.

4.4. Якщо є підстави вважати, що обліковий запис або пароль могли бути втрачені, скомпрометовані (стали відомі іншій особі) або змінені без участі користувача, про це відразу необхідно повідомити ВІТ.

4.5. Усі користувачі, яким для виконання службових функцій надається парольний доступ до ІС в Київській обласній прокуратурі, мають дотримуватися вимог цих Правил.

4.6. Під час створення облікового запису в будь-якій ІС користувачу встановлюється стартовий пароль, який повинен бути змінений користувачем на особистий, згідно вимог правил безпеки певною ІС.

4.7. Забороняється використовувати персональний комп'ютер з обліковим записом іншого працівника прокуратури.

5. Використання мережі Інтернет

5.1. Доступ до мережі Інтернет в Київській обласній прокуратурі надається лише для виконання службових обов'язків.

5.2. Доступ до мережі Інтернет є персоніфікованим.

5.3. Інформація щодо історії відвідування користувачами інформаційних ресурсів зберігається автоматично у вигляді лог-файлів на серверах Київської обласної прокуратури. Ця інформація може бути використана лише у службових цілях.

5.4. ВІТ може блокувати доступ до сайтів згідно з вимогами чинного законодавства України та рекомендаціями уповноважених державних органів.

5.5. При використанні доступу до мережі Інтернет користувач має уникати:

- завантаження з мережі будь-якого програмного забезпечення (винятки становлять оновлення Java та веб-браузерів, що обумовлено роботою єдиного реєстру досудових розслідувань (ЄРДР) та іншими інформаційними системами;

- відвідування, за винятком службової необхідності, сайтів, які пропагандують зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, війну, насильство, розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на права і свободи людини, здоров'я

населення, містять кіно- та відеопродукцію, комп'ютерні програми порнографічного характеру, твори, зображення або інші предмети порнографічного характеру;

- завантаження великих за обсягом (понад 1024 мб) файлів, що обмежує пропускну здатність загального каналу доступу до мережі Інтернет і сповільнює роботу інших користувачів та систем;

- завантаження на сайти в мережі Інтернет інформації з обмеженим доступом, або такої, що містить персональні дані;

- користування сайтами - «анонімайзерами» для прихованого відвідування сайтів, доступ на які обмежений адміністраторами ВІТ;

- здійснення доступу до мережі Інтернет з робочих ПК через особисті модеми та мобільні пристрої, як і їх особисте використання;

- відвідування сайтів, які пропонують встановити будь-яке ПЗ (наприклад, «оптимізатори для сайтів», «оновлювачі драйверів» тощо), і надання згоди на встановлення невідомого ПЗ;

- натискання банерів з «терміновими новинами», рекламними акціями, гарячими пропозиціями, онлайн лотереями тощо, що може призвести до прихованого встановлення небажаного і небезпечного ПЗ.

5.6. Отримані в мережі Інтернет матеріали слід використовувати з одержанням вимог законодавства. При цьому необхідно пам'ятати, що всі дії користувача в мережі Інтернет залишають електронний «слід», у зв'язку з цим необхідно уникати таких дій, які можуть завдати шкоди репутації Київської обласної прокуратури.

5.7. ВІТ у разі встановлення фактів систематичного порушення цих правил щодо роботи в мережі Інтернет, завантаження великих обсягів інформації може обмежувати швидкість або блокувати доступ конкретному користувачу, про що невідкладно повідомляється керівника відповідного структурного підрозділу.

6. Використання електронної пошти

6.1. Для виконання службових обов'язків працівниками Київської обласної прокуратури використовується виключно службова електронна пошта. Одночасно службова електронна пошта не може використовуватись поза межами виконання службових обов'язків. Усі повідомлення електронної пошти Київської обласної прокуратури в домені gp.gov.ua є власністю Офісу Генерального прокурора.

6.2. Службове листування здійснюється з абонентами, пошта яких розміщена на серверах, які перебувають у доменній зоні GOV.UA. Направлення службової електронної пошти на інші домени допустиме у крайніх випадках після консультацій із спеціалістами ВІТ.

6.3. Створення і налаштування службової електронної пошти здійснюється працівниками ВІТ.

6.4. Адреса (логін) електронної пошти може бути двох видів:

- за структурним підрозділом (напр. *secretariat@gp.gov.ua);*

- за прізвищем та ініціалами (напр. *ivanov.ii@gp.gov.ua).*

6.5. Електронна пошта структурного підрозділу створюється за письмовою заявкою безпосереднього керівника підрозділу з погодженням адреси скриньки. Доступ до неї може переходити від працівника до працівника в межах підрозділу з повідомленням ВІТ про зміну відповідальної за пошту особи. Під час такої передачі новий користувач має ініціювати зміну паролю до такої скриньки.

6.6. Персональна електронна пошта створюється за прізвищем та ініціалами працівника відповідно до правил транслітерації. Персональна поштова скринька не передбачає використання в колективних чи особистих цілях.

6.7. Розмір поштового листа в сукупності з додатками не може перевищувати 10 мб.

6.8. Поштова скринька має фіксований розмір. Для уникнення переповнення та забезпечення стабільного відправлення-приймання листів, користувач має регулярно перевіряти поштову скриньку, видаляти неактуальні листи та листи з великими за обсягами додатками. Це зменшує навантаження на поштовий сервер та ПК.

6.9. Необхідно постійно переглядати списки контактів, що зберігаються у користувача, і видаляти неактуальні та підозрілі, оскільки через контакти може відбуватися прихована розсилка комп'ютерних вірусів та спаму.

6.10. Службова електронна пошта не може використовуватися для відправки інформації з обмеженим доступом.

6.11. Користувач має утримуватись від відкривання неочікуваної і підозрілої пошти від невідомих відправників, особливо вкладених файлів та посилань. Такі листи необхідно видаляти відразу після отримання.

6.12. Якщо під час виконання службових обов'язків виникла потреба відправки повідомлення зі службової поштової скриньки іншого користувача (за його обов'язковим інформуванням), необхідно в повідомленні вказати своє власне ім'я.

6.13. При роботі з електронною поштою слід дотримуватися загальноприйнятих правил етикету, ретельно перевіряти повідомлення перед відправкою, особливо при спілкуванні з організаціями та відомствами. Необхідно пам'ятати, що повідомлення зі службової електронної пошти може бути інтерпретовано як офіційна позиція чи висловлювання Київської обласної прокуратури.

6.14. Доступ до створених, відправлених та отриманих повідомлень службової електронної пошти без дозволу користувача може бути здійснений відповідно до вимог чинного законодавства.

6.15. Усі користувачі, що мають службові облікові записи електронної пошти Київської обласної прокуратури мають дотримуватися вимог цих Правил.

7. Використання файлового сховища та мережевих папок

Файловий сервер призначений для зручної та швидкої колективної роботи з матеріалами. На ньому створені папки, у яких зберігається необхідна інформація в межах структурного підрозділу.

7.1. Створення папки для підрозділу здійснюється за заявкою керівника цього підрозділу (Виділений інформаційний ресурс).

7.2. Створення, надання доступу, налаштування прав доступу до папки здійснюється виключно спеціалістами ВІТ.

7.3. Вся інформація, що зберігається в мережевих папках, є власністю Київської обласної прокуратури.

7.4. При роботі з матеріалами в мережевих папках необхідно слідкувати, щоб не допустити зміни, видалення або заміни інших документів.

7.5. У мережевих папках не підлягають розміщенню:

- матеріали, які не стосуються робочого процесу (мультимедійна продукція, ігри тощо);

- програмне забезпечення, що містить комп'ютерні віруси та інші будь-які файли, що виконуються (з розширенням *.exe, *.com, *.bat, *.scr) та скрипти

(розширення *.vbs, *js, *.jse).

7.6. Видалення будь-яких файлів з папки підрозділу здійснюється за вказівкою керівництва цього підрозділу.

7.7. При роботі з мережевими папками не передбачено надання доступу до папки підрозділу працівникам іншого підрозділу або стороннім особам. Для забезпечення такого доступу для виконання службових обов'язків необхідно письмове звернення до ВІТ та згода відповідного керівника цього самостійного підрозділу.

7.8. Особа, яка здійснила навмисне знищення, часткове пошкодження або спотворення інформації, яка зберігається на файловому сервері, несе відповідальність згідно з законодавством.

8. Використання зв'язку на основі IP-телефонії

В органах прокуратури функціонує власна централізована система зв'язку на основі IP-телефонії виробництва компанії Cisco. Ця система зв'язку дозволяє здійснювати безкоштовні міжміські та внутрішні дзвінки в приміщеннях органів прокуратури; отримувати якісний, сучасний та захищений зв'язок. Також цей зв'язок дозволяє здійснювати не лише звичайні аудіодзвінки, але й проводити відеоконференції.

8.1. Для проведення телефонних розмов під час виконання службових обов'язків для економії бюджетних коштів рекомендовано використовувати мережу IP-телефонії (за наявності IP-телефону).

8.2. Встановлення, підключення та переміщення терміналів (IP-телефонів) здійснюється працівниками ВІТ за наявності технічних умов.

8.3. Абонентський номер у мережі IP-телефонії видається відповідно до єдиного номерного плану органів прокуратури України.

8.4. Абонентський номер і телефонний апарат закріплюється за кабінетом (в окремих випадках за посадою, або особою).

8.5. Додаткові сервіси IP-телефонії (переадресація дзвінків, номери швидкого виклику тощо) включені лише для телефонів керівників вищої ланки (від начальників управлінь). Для інших абонентів додаткові сервіси включаються за письмовою заявкою з обґрунтуванням, яка погоджується керівником самостійного підрозділу.

8.6. Зміна прізвища або номера абонента, внесення змін до довідників. корегування номерів швидкого виклику (на основі шаблону) здійснюються працівниками ВІТ.

8.7. У виняткових випадках допускається підключення до мережі IP-телефонії сторонніх терміналів (телефонів) після узгодження технічної можливості з працівниками ВІТ.

8.8. Під час користування IP-телефонією недопустимим є:

- використання зв'язку на основі IP-телефонії в особистих та не пов'язаних з виконанням службових обов'язків цілях;

- озвучення інформації з обмеженим доступом;

- перехоплення, прослуховування, запис, зберігання або публікація телефонних розмов без згоди всіх їх учасників, крім випадків, передбачених законодавством.

8.9. Не рекомендується використовувати зв'язок на основі IP-телефонії для озвучення і обговорення робочої та оперативної інформації, якщо в розмові беруть участь абоненти не IP-телефонії (внутрішні аналогові, міські, міжміські та мобільні телефони).

8.10. Телефонні апарати та супутнє обладнання є матеріальними цінностями органів прокуратури.

8.11. Усі абоненти, що користуються зв'язком на основі IP-телефонії в Київській обласній прокуратурі, мають дотримуватися вимог цих Правил.

9. Використання відеоконференцзв'язку (ВКЗ)

В органах обласної прокуратури використовується ВКЗ для проведення навчальних, організаційних та інших заходів.

9.1. Для проведення сеансів ВКЗ необхідно використовувати службові

системи відеозв'язку на основі IP-телефонії.

9.2. У разі відсутності службової системи ВКЗ допускається використання загальнодоступних систем (Skype, Zoom тощо), але слід пам'ятати, що ця інформація проходить через незахищені канали зв'язку і може бути використана третіми особами.

9.3. З метою забезпечення робочого процесу та уникнення витоку інформації службовий ВКЗ:

- використовується лише в службових цілях;
- не передбачений для озвучення інформації з обмеженим доступом.

9.4. Перехоплення, прослуховування, запис, зберігання або публікація сеансів ВКЗ не є повноваженням користувачів ВКЗ. У разі необхідності здійснення запису аудіо/відеоконференції про це повинні бути повідомлені всі учасники конференції та дати згоду на здійснення запису, крім випадків, передбачених законодавством.

9.5. Не рекомендується використовувати ВКЗ для озвучення і обговорення робочої та оперативної інформації, якщо в конференції беруть участь інші абоненти (представники сторонніх організацій, відомств тощо).

9.6. Усі користувачі ВКЗ в Київській обласній прокуратурі мають дотримуватися вимог цих Правил.

Відділ інформаційних технологій
Київської обласної прокуратури