

ЗАТВЕРДЖЕНО

Наказ директора Центрального
державного електронного архіву
України

28.10.2015 № 91

ІНСТРУКЦІЯ

користувача інформаційно-телекомунікаційної системи Центрального державного електронного архіву України

І. Загальні положення

1.1. Ця Інструкція встановлює загальні положення організації роботи працівників Центрального державного електронного архіву України (далі – користувачів) в інформаційно-телекомунікаційній системі архіву (далі – ІТС).

1.2. ІТС є програмно-технічним комплексом, який забезпечує функціонування єдиного інформаційного середовища Центрального державного електронного архіву України (далі – ЦДЕА України).

1.3. Робота користувачів в ІТС, діяльність адміністрації ІТС та технічного персоналу ІТС здійснюється відповідно до Конституції України, законів України «Про Національний архівний фонд та архівні установи», «Про інформацію», «Про внесення змін до деяких законодавчих актів України щодо посилення протидії незаконному обігу архівних документів», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну програму інформатизації», «Про електронні документи та електронний документообіг», «Про захист персональних даних», Положення про Центральний державний електронний архів України, інші нормативно-правові акти в сфері легалізації комп'ютерного програмного забезпечення, архівної справи, роботи з електронними документами та захисту інформації, розподілу обов'язків між директором і заступниками директора ЦДЕА України, положень про структурні підрозділи архіву, посадових інструкцій працівників ЦДЕА України.

1.4. У цій Інструкції терміни вживаються в такому значенні:

– адміністрація ІТС – працівники ЦДЕА України, які відповідають за прийняття рішень з питань роботи, розвитку та модернізації ІТС, а саме директор та начальник відділу інформаційних технологій архіву;

– інформаційні ресурси (далі – ресурси) – логічні структури надання даних для користувачів, доступні в ІТС;

– програмне забезпечення – всі або частина програм, процедур, правил і відповідної документації системи обробки інформації;

– робоча станція – апаратно-програмний комплекс, який підключений до ІТС та надає можливість використовувати мережеві ресурси та сервіси ІТС;

– спроба несанкціонованого доступу – дії, що кваліфікуються як факт спроби порушника вплинути на роботи ІТС з метою отримання, зміни або знищення інформації минаючи визначену політику безпеки в ЦДЕА України, у тому числі й цією Інструкцією;

– технічний персонал ІТС – працівники ЦДЕА України, які відповідають за обслуговування, моніторинг технічних, програмних та інформаційних складових ІТС відповідно до своїх посадових обов'язків;

– трафік – обсяг інформації, що передається через ІТС за певний проміжок часу.

II. Порядок підключення до ІТС

2.1. Підключення робочих станцій до ІТС здійснюється технічним персоналом ІТС.

2.2. Користувач допускається до роботи в ІТС тільки після проходження інструктажу з організації роботи в ІТС під розпис, що фіксується у картці обліку встановлених комп'ютерних програм у відповідності до Постанови Кабінету Міністрів України від 10.09.2003 № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади».

2.3. Доступ користувача до ІТС забезпечується за допомогою логіна і пароля.

2.3.1. Первинний доступ користувача до ІТС забезпечує адміністратор ІТС який надає користувачу логін і пароль. Логіном користувача для доступу до ІТС є його прізвище, яке переведено з українського написання на латиницю у відповідності до «Таблиці транслітерації українського алфавіту латиницею», затвердженого постановою Кабінету міністрів України від 27.01.2010 № 55.

2.3.2. При першому вході до свого облікового запису в ІТС користувач на вимогу системи зобов'язаний змінити пароль, який буде відомий тільки йому.

III. Права і обов'язки користувача

3.1. Користувач несе повну відповідальність за всі дії, що здійснюються ним у ІТС.

3.2. Користувач має право:

3.2.1. Отримувати доступ до наявних ресурсів ІТС у межах, дозволених адміністрацією ІТС.

3.2.2. Звертатися за довідковою інформацією та консультацією до технічного персоналу ІТС у межах його компетенції.

3.2.3. Отримати доступ до послуг електронної пошти та інших служб ІТС для виконання посадових обов'язків. Режим доступу до мережі Інтернет визначається адміністрацією ІТС відповідно до посадових обов'язків кожного користувача індивідуально. Доступ може бути наданий з обмеженням у часі та періоді користування послугами.

3.3. Користувач зобов'язаний:

3.3.1. Виконувати всі вимоги даної Інструкції.

3.3.2. Виконувати правила техніки безпеки під час роботи в ІТС.

3.3.3. Зберігати всі документи, створені під час його роботи, у відповідному каталозі на сервері ЦДЕА України, що створюється технічним персоналом ІТС.

3.3.4. Не розголошувати ідентифікаційну інформацію, яка використовується для доступу до ресурсів ІТС (паролів та інших кодів авторизованого доступу).

3.3.5. Повідомляти про всі помічені спроби несанкціонованого доступу до ресурсів ІТС та дії, що можуть призвести до порушення або зупинки роботи ІТС.

3.4. Користувачу забороняється:

3.4.1. Використовувати ІТС у цілях, які не відповідають завданням, визначеним у посадовій інструкції користувача.

3.4.2. Надавати доступ до ІТС стороннім особам у будь-якій формі, а також надавати доступ до каналів зв'язку користувачам інших мереж.

3.4.3. Розповсюджувати у комп'ютерних мережах інформацію (серійні номери ліцензійного програмного забезпечення, саме програмне забезпечення, файли даних і т.п.), що використовується в ІТС і є інтелектуальною власністю сторонньої особи та захищена законодавством щодо авторського права.

3.4.4. Створювати й підтримувати засобами ІТС будь-які ресурси, зміст, цілі та завдання яких не відповідають завданням, визначеним у посадовій інструкції користувача.

3.4.5. Публікувати та розсилати інформацію, що порушує чинне законодавство України (порнографічні матеріали, пропаганду насилля, расизму, релігійної ненависті; розповсюдження, виготовлення та застосування наркотичних і небезпечних речовин, політичну та релігійну пропаганду тощо).

3.4.6. Здійснювати несанкціоновану розсилку електронних листів й електронних повідомлень адресатам, які не давали згоди на їх отримання.

3.4.7. Фальсифікувати зворотну адресу електронної пошти, IP-адресу робочого місця, адреси, що використовуються в інших мережевих протоколах, під час передавання даних у комп'ютерні мережі, а також використовувати ідентифікаційні дані (імена, адреси, телефони і т.п.) третіх осіб, крім випадків, коли ці особи уповноважили користувача на таке використання.

3.4.8. Здійснювати спроби несанкціонованого або неправомірного доступу до ресурсів ІТС, проводити або брати участь у мережевих атаках і мережевому зламі, за виключенням випадків, коли подібні дії проводиться з дозволу власника або адміністратора даного ресурсу (наприклад, в межах перевірки системи безпеки).

3.4.9. Чинити дії, направлені на фізичне пошкодження складових ІТС (комп'ютерів, іншого обладнання чи програмного забезпечення).

3.4.10. Створювати, використовувати та розповсюджувати шкідливе програмне забезпечення (комп'ютерні віруси, мережеві «хробаки», «троянські коні», руткіти тощо), у тому числі спрямовані на отримання несанкціонованого доступу до будь-яких підсистем і служб ІТС або на порушення цілісності цих складових ІТС.

3.4.11. Чинити будь-які інші дії, визначені чинним законодавством України у сфері захисту інформації як злочини.

3.5. Користувач повинен знати:

3.5.1. ІТС створюється на основі програмного забезпечення, що визначається адміністрацією ІТС, у тому числі вільного програмного забезпечення та відкритих форматів даних.

3.5.2. З метою забезпечення інформаційної безпеки:

3.5.2.1. Зміст електронної пошти користувача може бути проаналізовано адміністратором ІТС на наявність шкідливого програмного коду та відповідність цілям та завданням визначеним в посадовій інструкції користувача.

3.5.2.2. Усі дії користувача протоколюються та можуть бути проаналізовані адміністратором ІТС та технічним персоналом ІТС на відповідність цілям та завданням визначеним в посадовій інструкції користувача.

3.5.2.3. Технічний персонал ІТС зобов'язаний контролювати трафік, адресацію та джерела повідомлень, що надходять до ІТС та виходять із неї, виявляти та ідентифікувати користувачів ІТС, які здійснюють спроби заподіяння шкоди або збитків інформаційним, обчислювальним, технічним та мережевим ресурсам ІТС, а також виявляти спроби несанкціонованого доступу.

3.5.3. Працівникам адміністративно-господарської частини, технічним працівникам, особам, які здійснюють ремонтні та будівельно-монтажні роботи, забороняється порушувати цілісність кабельних систем і кабельних каналів ІТС, виконувати демонтаж мережевого обладнання без погодження з адміністрацією ІТС. У випадку виконання робіт сторонніми установами, працівник ЦДЕА України, який курує будівельно-монтажні або ремонтні роботи, несе персональну відповідальність за збереження та цілісність кабельних систем і обладнання ІТС.

3.5.4. Адміністрація ІТС може обмежувати доступ до ІТС або її ресурсів у випадку порушення вимог цієї Інструкції.

ВІДПОВІДАЛЬНІСТЬ

Порушення вимог цієї Інструкції може призвести до дисциплінарної, громадянської, адміністративної, кримінальної та іншої відповідальності, передбаченої чинним законодавством України.