ЗАТВЕРДЖЕНО

Розпорядження голови
районної у місті ради
від 05 лютого 2025 року № 27-р

ІНСТРУКЦІЯ
про попередження кібератак під час роботи з електронно-обчислювальною технікою та інформаційно-телекомунікаційними системами

І. Загальні вимоги

Працюючи з інформаційними ресурсами виконкому районної у місті ради, кожен працівник зобов'язаний:

1.1 забезпечувати, в залежності від своїх посадових обов'язків, захист від несанкціонованого доступу до інформації, до якої він має санкціонований доступ;

1.2 не брати участь у процесах несанкціонованого доступу до інформації, що належить іншим працівникам;

1.3 не використовувати інформацію, що стала йому відома під час виконання своїх функціональних обов'язків, не за прямим призначенням;

1.4 у разі порушення встановлених правил доступу іншими працівникам повідомляти про це керівника структурного підрозділу, відділ інформаційної безпеки та електронного документообігу.

ІІ. Обов’язки працівників під час роботи в автоматизованих інформаційних системах

2.1. Під час роботи в автоматизованій інформаційній системі виконкому районної у місті ради працівник зобов’язаний:

2.1.1 зберігати у таємниці паролі доступу до системи (систем);

2.1.2 надійно зберігати фізичні ключі (ідентифікатори) доступу;

2.1.3 змінювати особисті паролі на вимогу відділу інформаційної безпеки та електронного документообігу;

2.1.4 при випадковому отриманні доступу до чужої конфіденційної інформації (збій механізмів захисту, аварії, недбалість працівників тощо) припинити будь-які дії в системі та негайно повідомити керівника структурного підрозділу, відділ інформаційної безпеки та електронного документообігу.

2.2. Повідомляти керівника структурного підрозділу, відділ інформаційної безпеки та електронного документообігу про відомі канали витоку інформації, способи та засоби обходу або руйнування механізмів захисту.

2.3. Під час роботи в автоматизованій інформаційній системі виконкому районної у місті ради працівнику забороняється (крім випадків, передбачених посадовими інструкціями або іншими нормативно-правовими актами):

2.3.1 записувати у будь-якому доступному вигляді або вимовляти вголос відомі користувачеві паролі;

2.3.2 реєструватися та працювати у системі під чужим ідентифікатором та паролем;

2.3.3 передавати ідентифікатори та паролі будь-кому;

2.3.4 залишати без нагляду робоче місце протягом сеансу роботи;

2.3.5 дозволяти робити будь-які дії із закріпленим за користувачем комплектом програмно-апаратних засобів іншим особам;

2.3.6 несанкціоновано змінювати або знищувати дані чи програми у мережі чи носіях;

2.3.7 залишати без нагляду носії інформації;

2.3.8 використовувати комп'ютерну техніку не за прямим призначенням;

2.3.9 займатися дослідженням обчислювальної мережі;

2.3.10 ігнорувати системні повідомлення та попередження про помилки;

2.3.11 несанкціоновано встановлювати на електронно-обчислювальну техніку будь-які додаткові програмні, апаратні компоненти та пристрої;

2.3.12 копіювати на зовнішні носії будь-яке програмне забезпечення та файли даних;

2.3.13 використовувати для передачі інформації обмеженого доступу непризначені для цього засоби і канали зв'язку.

III. Системи, ресурси, додатки, програмні застосунки, що заборонені до використання працівниками на робочих місцях

При роботі на електронно-обчислювальній техніці працівникам забороняється:

3.1 використовувати неліцензовані сервіси VPN (Virtual Private Network), що дозволяють об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів Internet-адресації, або інші, аналогічні, програмні рішення, що дозволяють створювати віртуальні мережі у фізичному каналі мережі Internet;

3.2 використовувати месенджер Telegram для обміну текстовими, голосовими, відеоповідомленнями, фотографіями, файлами, що містять інформацією, яка стосується професійної діяльності працівника, або виконання працівником його посадових обов'язків.

IV. Дії працівників під час роботи в корпоративній поштовій системі

При роботі в корпоративній поштовій системі виконкому районної у місті ради працівнику забороняється:

4.1 використовувати корпоративну електронну пошту в особистих цілях;

4.2 проводити розсилку листів невиробничого характеру, матеріалів рекламного та розважального характеру;

4.3 проводити розсилку шкідливих програм або файлів, з шкідливим програмним забезпеченням;

4.4 використовувати електронну пошту для передачі матеріалів великого обсягу (більше 256 Мб);

4.5 використання сторонніх поштових сервісів Інтернету (mail.ru, yandex.ru тощо);

4.6 публікувати свою корпоративну адресу або адреси інших працівників установи на загальнодоступних Інтернет ресурсах (форуми, конференції тощо), якщо це не пов'язано з виконання посадових обов'язків;

4.7 відкривати листи, електронна адреса яких закінчується на «.ru»;

4.8 переходити за посиланнями, вкладеними в електронні листи, що мають ознаки небезпечних електронних листів;

4.9 завантажувати, відкривати, пересилати виконувані файли (з розширеннями – .exe, .dll, .pif, .ppsx тощо);

4.10 відкривати, пересилати, видаляти небезпечні електронні листи (крім випадків, передбачених посадовими інструкціями).

V. Дії працівників при виявленні небезпечних електронних листів

5.1. При виявленні небезпечних електронних листів працівник зобов'язаний негайно повідомити керівника структурного, відділ інформаційної безпеки та електронного документообігу.

5.2. Ознаки небезпечних електронних листів:

5.2.1 адреса, з якої надійшов лист закінчується на «.ru»;

5.2.2 спостерігається спроба отримати ваші персональні дані, наприклад, дані для входу в обліковий запис на якомусь сайті;

5.2.3 лист спонукає перейти за посиланням, не пояснюючи, куди воно веде;

5.2.4 до листа від невідомого відправника прикріплено файл(и).

VI. Дії працівників при виникненні непередбачуваних обставин

У разі виникнення підозри ураження шкідливим програмним забезпеченням електронно-обчислювальної техніки чи інформаційно-телекомунікаційних систем слід терміново повідомити керівника структурного підрозділу, відділ інформаційної безпеки та електронного документообігу для координації подальших дій та усунення негативних наслідків.

В. о. керуючого справами виконкому –
заступник голови районної у місті
ради з питань діяльності виконавчих
органів ради Надія СТАВИЦЬКА