ЗАТВЕРДЖЕНО

Розпорядження начальника

обласної військової адміністрації

27 червня 2025 року № 373

ПРАВИЛА

роботи працівників апарату Волинської обласної державної

адміністрації на персональних комп’ютерах,

у корпоративній мережі та мережі «Інтернет»

1. Загальні положення

1. Правила роботи працівників апарату Волинської обласної державної адміністрації на персональних комп’ютерах, у корпоративній мережі та мережі «Інтернет» (далі – Правила) розроблені з метою організації та врегулювання інформаційних процесів при роботі на персональних комп’ютерах (далі – ПК), у корпоративній мережі та мережі «Інтернет» чіткої та злагодженої взаємодії працівників завдяки автоматизації процесів передавання (приймання), обробки, відображення, документування інформації.

2. Основні поняття та терміни, що використовуються Ву Правилах, мають такі визначення:

1) захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

2) інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

3) комплексна система захисту інформації – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

4) кіберінцидент – це подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема і внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (зокрема зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

5) кіберзагроза – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

6) індикатори кіберзагроз – це показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози.

3. Дотримання Правил поліпшить:

1) регламентацію діяльності працівників апарату обласної державної адміністрації при використанні персональних комп’ютерів;

2) використання ресурсів корпоративної мережі, мережі «Інтернет»;

3) підтримку необхідного рівня захисту інформації, її збереження і дотримання прав доступу до інформації, встановлених її власником;

4) інформаційну взаємодію працівників апарату.

2. Загальні аспекти роботи на персональних комп’ютерах

1. Комп’ютерна техніка, електронна поштова скринька на офіційному домені обласної державної адміністрації, доступ до інформаційних систем та ресурсів надається працівникам апарату (далі – Користувач) виключно для виконання своїх посадових обов’язків.

2. Для організації робочого місця користувачу надається ноутбук або персональний комп’ютер (ПК), який може бути укомплектований таким чином (за наявності обладнання):

1) системний блок;

2) монітор;

3) маніпулятори типу миша, клавіатура;

4) блок безперебійного живлення;

5) інша оргтехніка (принтер, сканер, гарнітура тощо) в разі службової потреби.

Програмне забезпечення використовується тільки за наявності ліцензій або те, що є у вільному доступі з офіційних джерел. Пакет програмного забезпечення визначають відповідальні особи в повному обсязі для виконання посадових обов’язків користувачів.

3 Кожен Користувач отримує персональний ідентифікатор (логін і пароль), що використовується для доступу:

1) до робочого середовища на персональному комп’ютері;

2) до файлового сховища;

3) до системи електронного документообігу «АСКОД»;

4) на офіційний сайт обласної державної адміністрації (за службової потреби).

4. Користувач несе повну відповідальність за дії та/або бездіяльність, що привели до розголошування, втрати, крадіжки тощо його персонального ідентифікатора та іншої інформації, що індивідуалізує Користувача, а також за будь-які дії та/або бездіяльність третіх осіб, що використовують ідентифікатор Користувача.

5. Користувач несе повну персональну відповідальність за інформацію, опубліковану, надіслану від його імені.

6. Користувач зобов’язаний дотримуватися конфіденційності своїх облікових даних і вживати заходів, спрямованих на їх захист від розголошення, втрати, крадіжки.

7. У разі втрати пароля чи бажання його зміни Користувачеві дається новий пароль (який повинен містити довжину не менше 6 символів, великі, маленькі літери латинського алфавіту, цифри, спеціальні символи) після звернення до відділу інформаційно-комунікаційних систем апарату обласної державної адміністрації.

8. Підключення, відключення, заміна або налаштування елементів ПК здійснюється виключно відповідальними особами.

9. Користувач несе персональну відповідальність за збереження комп’ютерної техніки, наданої йому в користування для виконання своїх службових обов’язків.

10. Усі працівники, які використовують ПК для виконання своїх службових обов’язків в апараті обласної державної адміністрації, зобов’язані дотримуватись цих Правил і бути ознайомлені з ними під підпис.

11. Правила є обов’язковими також і для осіб, яким для виконання своїх службових обов’язків відповідальними особами надано ПК для тимчасового використання або які підключають свої персональні комп’ютери до локальної обчислювальної мережі.

12. У разі виникнення будь-яких апаратних чи системних несправностей ПК Користувач зобов’язаний негайно припинити роботу і викликати відповідальну особу.

13. У разі виявлення кіберінцидентів відповідальними особами, які використовують індикатори кіберзагроз, Користувач зобов’язаний негайно надати доступ до ПК для усунення кіберзагроз.

14. Користувачам персональних комп’ютерів забороняється:

1) зберігати та запускати на ПК будь-яке стороннє програмне забезпечення без відома відповідальних осіб;

2) використовувати неліцензійне програмне забезпечення;

3) надавати можливість використання свого комп’ютера іншим користувачам, якщо це не викликано службовою потребою;

4) використовувати комп’ютерну техніку в особистих цілях;

5) надавати адресу службової скриньки електронної пошти для отримання інформації неслужбового характеру;

6) вилучати, встановлювати чи змінювати будь-які апаратні компоненти комп’ютерної техніки, змінювати конфігурації наявного програмного забезпечення;

7) самостійно виконувати будь-які ремонтні та профілактичні роботи ПК;

8) самостійно здійснювати переміщення комп’ютерної техніки;

9) підключати до ПК особисті носії даних (особисті флешки, телефони, з’ємні жорсткі диски);

10) вводити, обробляти та зберігати конфіденційну інформацію, інформацію з грифом «Для службового користування», інформацію, що є державною таємницею на ПК, на яких не побудована відповідна комплексна система захисту інформації.

15. Після завершення робочого дня користувачі зобов’язані вимкнути персональний комп’ютер, іншу комп’ютерну техніку з мережі електроживлення.

16. Користувачу необхідно постійно і неухильно удосконалювати свої знання і навички роботи в інформаційному середовищі методами підвищення кваліфікації та самоосвіти (приклад – Дія. Цифрова освіта).

3. Права та обов’язки відповідальних осіб та користувачів

1. Права і обов’язки відповідальних осіб

Відповідальні особи мають право:

1) у разі зловживання корпоративною мережею, мережею «Інтернет» частково або повністю усувати порушників від користування нею;

2) видаляти програмне забезпечення, що порушує роботу корпоративної мережі або неліцензійне (піратське) програмне забезпечення;

3) видаляти особисту інформацію користувачів, що не відноситься до службової та загромаджує вільний дисковий простір персональних комп’ютерів та спільних мережевих ресурсів;

4) змінювати паролі користувачів у разі виявлення фактів компрометації даних автентифікації;

5) вилучати комп’ютерну техніку в разі виявлення кіберінцидентів для аналізу та усунення причин і наслідків подій;

6) давати вказівки щодо роботи в корпоративній мережі, локальній обчислювальній мережі (далі − ЛОМ), які не суперечать вимогам цих Правил;

7) обмежувати доступ мережі «Інтернет» або відключати від неї в разі порушень цих Правил.

8) блокувати доступ до сайтів та інформаційних ресурсів, що несуть у собі розважальний характер.

2. Відповідальні особи зобов’язані:

1) обмежувати доступ працівників у приміщення, де встановлено сервери і комутаційне обладнання корпоративної мережі;

2) здійснювати контроль за дотриманням структури корпоративної мережі;

3) реалізовувати організаційні та технічні заходи для налагодження політики безпеки домена та мережевого екрану;

4) реагувати на підозрілу активність користувачів (може здійснюватися без відома користувача шкідливим програмним забезпеченням), використовуючи системи мережевого моніторингу;

5) вживати організаційних і технічних заходів для припинення спроб несанкціонованого доступу до комп’ютерної техніки із зовнішніх мереж.

3. Права і обов’язки користувача

Користувач має право:

1) на доступ до всіх ресурсів корпоративної мережі, ЛОМ, інформаційних систем у межах виконання посадових обов’язків та відповідно до цих Правил;

2) звертатися за інформацією і консультацією до відповідальних працівників, що обслуговують корпоративну мережу, ЛОМ, інформаційні системи.

4. Користувач зобов’язаний:

1) ознайомитися з цими Правилами під підпис;

2) використовувати ресурси корпоративної мережі, ЛОМ, інформаційних систем виключно в цілях, пов’язаних з виконанням службових обов’язків;

3) виконувати вимоги відповідальних осіб, що не суперечать цим Правилам;

4) дотримуватися правил техніки безпеки при роботі з комп’ютерною технікою;

5) забезпечувати нерозголошення даних автентифікації (логіни та паролі), що використовуються для доступу до ПК, ресурсів корпоративної мережі, ЛОМ, мережі «Інтернет», інформаційних систем;

6) перешкоджати несанкціонованому і недобросовісному використанню ресурсів корпоративної мережі, ЛОМ, інформаційних систем;

7) користуватися антивірусними програмами;

8) повідомляти відповідальних осіб про локальні кіберінциденти;

9) звертатися до відповідальних осіб у разі потреби проведення робіт з ПК, у корпоративній мережі, мережі «Інтернет» та інформаційних ресурсах;

10) постійно вдосконалювати свої знання і навички роботи з комп’ютерною технікою, в корпоративній мережі та мережі «Інтернет», оскільки у будь-якій системі найслабшою ланкою захисту є користувач;

11) належно експлуатувати комп’ютерну техніку, запобігати попаданню на комп’ютерну техніку чужорідних речовин (рідин, крихт тощо).

4. Відповідальність за невиконання правил

1. Відповідальні особи несуть відповідальність за:

1) організацію управління корпоративною мережею;

2) функціонування корпоративної мережі загалом;

3) функціонування базових сервісів корпоративної мережі;

4) порушення функціонування корпоративної мережі внаслідок некоректного управління маршрутизацією;

5) встановлені права доступу до ПК у ЛОМ;

6) працездатність комп’ютерної техніки і устаткування ЛОМ, працездатність і фізичний стан ліній зв’язку і інших засобів комунікацій усередині корпоративної мережі;

7) порушення функціонування відповідних сегментів корпоративної мережі.

2. Користувачі несуть відповідальність за:

1) навантаження корпоративної мережі та мережі «Інтернет» діяльністю, що не несе службової потреби;

2) порушення функціонування корпоративної мережі;

3) інформацію, що знаходиться на ПК у ЛОМ, які входять до корпоративної мережі, і за діяльність, що ведеться на цих ПК;

4) зміст даних, що передаються через корпоративну мережу;

5) завантаження вільного мережевого та локального дискового простору даними, що не несуть службової потреби;

6) інформацію опубліковану, надіслану від його імені, використовуючи персональний ідентифікатор;

7) недотримання цих Правил.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_