ЧОРТКІВСЬКА РАЙОННА ДЕРЖАВНА АДМІНІСТРАЦІЯ ТЕРНОПІЛЬСЬКОЇ ОБЛАСТІ

ЧОРТКІВСЬКА РАЙОННА ВІЙСЬКОВА АДМІНІСТРАЦІЯ ТЕРНОПІЛЬСЬКОЇ ОБЛАСТІ

РОЗПОРЯДЖЕННЯ

від _____ 20__ року м. Чортків № _____

Про затвердження політики безпеки локальних мереж з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання

Відповідно до законів України «Про електронні комунікації», «Про захист персональних даних» та протоколу № 1 від 22 лютого 2023 року наради при заступнику начальника обласної військової адміністрації з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) щодо забезпечення безпеки мереж з доступом до Інтернету в районній військовій адміністрації:

1. Затвердити політику безпеки локальних мереж з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання в районній військовій адміністрації, що додається.

2. Визначити ВОЛОХ Оксану Тимофіївну, головного спеціаліста відділу забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації – відповідальною за політику безпеки локальних мереж з доступом до Інтернету в Чортківській районній військовій адміністрації.

3. У разі відсутності уповноваженої особи у зв’язку з тимчасовою непрацездатністю, перебуванням у відпустці та з інших причин, її обов’язки виконує головний спеціаліст відділу забезпечення взаємодії з органами

місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації ПАВЛЮК Андрій Олексійович.

4. Структурним підрозділам районної військової адміністрації (із статусом юридичної особи публічного права):

1) визначити відповідальну особу за політику безпеки локальних мереж з доступом до Інтернету;

2) ознайомитись з політикою безпеки локальних мереж з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання;

3) забезпечити неухильне дотримання політики безпеки використання локальної мережі з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання;

4) доручити призначеному працівнику, що відповідальний за політику охорони локальних мереж з доступом до Інтернету, перевірку обладнання на наявність кіберзагроз;

5) інформувати відділ забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації про звільнення/переведення працівників підрозділу районної військової адміністрації для забезпечення вимог політики безпеки локальних мереж з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання.

5. Контроль за виконанням даного розпорядження покласти на заступника начальника районної військової адміністрації згідно з розподілом обов’язків.

Начальник військової адміністрації **Володимир ШИПІТКО**

Михайло Демчук

Володимир Коцюк

Володимир Олійник

Оксана Волох

ЗАТВЕРДЖЕНО

Розпорядження начальника
районної військової адміністрації

_____2023 № _____

ПОЛІТИКА
безпеки локальних мереж з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання районної військової адміністрації

1. Загальні положення

1.1 Політика безпеки вводиться для безпеки використання локальних мереж з доступом до Інтернету та автоматизованих робочих місць районної військової адміністрації.

1.2 Політика безпеки поширюється та є обов'язковою до виконання всіма працівниками Чортківської районної військової адміністрації.

1.3 Політика безпеки визначає права і обов'язки як користувачів комп'ютерного обладнання, так і відповідального спеціаліста відділу забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації.

1.4 Локальна комп'ютерна мережа (надалі - Мережа) - це система програмно-апаратних ресурсів, які використовуються для вирішення задач інформаційного забезпечення та збільшення продуктивності роботи працівників, швидкості опрацювання та проходження документів. Апаратна частина цієї системи складається з комунікаційного обладнання, серверів та персональних комп'ютерів (ПК), які під’єднані до Мережі.

1.5 Користувачі, які працюють на під’єднаних до Мережі персональних комп'ютерах, є користувачами локальної комп'ютерної мережі (надалі – користувачі мережі).

1.6 Грубе або систематичне порушення користувачем цієї політики безпеки може служити підставою для застосування дисциплінарної відповідальності.

2. Обов'язки та права працівників відділу забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації

2.1 Підтримка працездатності та розширення Мережі.

2.2 Формування системної політики роботи Мережі, визначення принципів і правил конфігурації мережевого програмного забезпечення.

2.3 Контроль за виконанням користувачами дійсної політики безпеки локальної мережі з доступом до Інтернету, автоматизованих робочих місць та серверного обладнання і інформування керівництва районної військової адміністрації, щодо її порушення.

2.4 Право використовувати необхідне програмне забезпечення для контролю за використанням користувачами ресурсів Мережі та за виконанням ними пунктів даної політики безпеки.

2.5 Вдосконалення роботи обладнання та програмного забезпечення загального користування для підвищення ефективності виконання користувачами їх службових обов'язків.

2.6 Надання користувачам інформації необхідні для роботи на комп'ютерному обладнанні загального користування.

2.7 Проводення серед користувачів роз'яснювальної роботиу з питань інформаційної безпеки.

2.8 Доведення до відома користувачів правил роботи на конкретному обладнанні.

2.9 Не розголошення інформації, отриманої в ході виконання службових обов'язків, яка не має прямого відношення до виконуваних обов'язків.

3. Обов'язки та права користувачів

3.1 Користувачі зобов'язані:

3.1.1 ознайомитися з цією політикою безпеки до початку роботи на комп'ютерному обладнанні;

3.1.2 регулярно (не менше 3 разів на день) переглядати свою електронну скриньку на наявність нових повідомлень та видаляти небажану пошту;

3.1.3 використовувати обчислювальну та оргтехніку і програмне забезпечення виключно для діяльності, передбаченої виробничою необхідністю та посадовими інструкціями;

3.1.4 дбайливо ставитися до обладнання, дотримуватися правил його експлуатації;

3.1.5 сприяти співробітникам відділу забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації у виконанні ними своїх службових обов'язків, у разі необхідності - надавати доступ до ПК;

3.1.6. повідомляти працівників відділу забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації про помічені випадки порушення інформаційної безпеки (несанкціонований доступ до обладнання та інформації, несанкціоноване спотворення чи знищення інформації) також виявлені несправності обчислювальної техніки та оргтехніки, недоліки в роботі програмного забезпечення загального користування;

3.1.7 тримати у таємниці свої паролі доступу до ресурсів Мережі. Щоквартально видаляти власні не потрібні в роботі файли з елекронної скриньки та ПК.

3.2 Користувачам забороняється:

3.2.1 здійснювати дії, які перешкоджають нормальній працездатності комунікаційного чи іншого обладнання Мережі, а також вмикати або вимикати його без узгодження з відділом забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації;

3.2.2 заважати нормальній працездатності мережевих служб, інших ПК у Мережі;

3.2.3 використовувати обладнання або програмне забезпечення, яке приводить до недоцільного зниження пропускної здатності Мережі, або її окремих вузлів;

3.2.4 здійснювати несанкціонований доступ до захищених паролями мережевих ресурсів (принтерів, дисків із файлами, тощо), які не дозволені даному користувачеві для використання власником цього ресурсу;

3.2.5 використовувати програми підбору паролів до інших комп'ютерів Мережі;

3.2.6 підключатися до серверів та інших персональних комп’ютерів, використовуючи чужий логін та пароль;

3.2.7 займатися створенням або розповсюдженням будь-яких типів комп'ютерних вірусів;

3.2.8 змінювати конфігурацію параметрів протоколу TCP/IP ПК (зокрема IP-адреси);

3.2.9 використовувати устаткування для діяльності, не обумовленої виробничою необхідністю та посадовою інструкцією;

3.2.10 підключати до локальної мережі нові комп'ютери та обладнання без погодження з відділом забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації;

3.2.11 видаляти файли інших користувачів на ПК;

3.2.12 надавати доступ до комп'ютерного обладнання стороннім користувачам;

3.2.13 використовувати ресурси Інтернет та електронної пошти з метою масової розсилки електронних повідомлень комерційного, рекламного і іншого характеру, які не пов'язані з виконанням посадових обов’язків;

3.2.14 здійснювати несанкціонований доступ до ресурсів Інтернет, які захищені (паролями чи ін.), і до яких у користувача немає дозволу для доступу;

3.2.15 здійснювати тривале накопичення великих обсягів об’ємних файлів, що безпосередньо впливає на якість роботи встановленого програмного забезпечення;

3.2.16 використовувати безкоштовні зовнішні поштові ресурси та передавати ними службову інформацію;

3.2.17 здійснювати завантаження аудіо і відео файлів, так само як і їх потокові трансляції з мережі Інтернет;

3.2.18 проводити реєстрацію на Інтернет - ресурсах із наданням робочої поштової адреси.

3.3 Користувачам дозволяється:

3.3.1 отримувати доступ до мережі Інтернет, визначених баз даних, файлового серверу та інших ресурсів районної військової адміністрації, відповідно до заяви про надання повноважень завіреної керівництвом структурного підрозділу в якому працює користувач;

3.3.2 подавати заявку на обслуговування або ремонт обладнання у разі виникнення зауважень, щодо його функціонування;

3.3.3 вносити пропозиції щодо встановлення безкоштовного та придбання

комерційного програмного забезпечення загального користування;

3.3.4 отримувати консультацію у спеціалістів відділу забезпечення взаємодії з органами місцевого самоврядування, організаційної роботи та цифровізації районної військової адміністрації по роботі з комп'ютерним обладнанням і програмним забезпеченням загального користування, з питань комп'ютерної безпеки;

3.3.5 вносити пропозиції щодо зміни цих правил.

4. Політика безпеки

4.1. Управління оновленнями програмного забезпечення:

4.1.1 постійно слідкувати за версіями операційної системи, системи управління контентом (CMS), менеджера пакетів, фреймворків або іншого ПЗ, що забезпечують роботу веб-ресурсу, регулярно оновлювати їх.

4.2. Перевірка адрес веб-сайтів, а також їхні сертифікати:

4.2.1 уважно перевіряти веб-сайти, які відвідуються, якщо вони будуть вам підозрілі – не вказувати там жодних своїх даних;

4.2.2 у разі необхідності введення автентифікаційних даних переконатися, що з'єднання зашифроване. На це вказує адреса, яка починається з https:// та іконка закритого замка, також перевіряти сертифікат веб-сайту (достатньо натиснути на замок).

4.3. Антивірусний захист:

4.3.1 встановлення та оновлення ліцензійних антивірусів;

4.3.2 здійснювати оновлення регулярно та автоматично;

4.3.3 надавати можливість антивірусу регулярно (наприклад, шомісячно) здійснювати перевірки комп’ютерних файлів.

4.4. Використання надійних паролів:

4.4.1 виключити використання скрізь одних і тих самих паролів, змінювати їх регулярно;

4.4.2 не зберігати паролі в Інтернет-браузері;

4.4.3 використання двох факторної автентифікації там, де це можливо.

4.5. Використання в роботі Мережі Інтернет в тому числі WIFI –мережі виключно ті, які підключені в районній військовій адміністрації:

4.5.1 не відправляєти важливу інформацію через недовірені та незнайомі мережі.

5. Відповідальність за порушення норм Інструкції

5.1 Відповідальність за порушення Інструкції наступає відповідно до вимог чинного законодавства України.

5.2 У випадку порушення даної Інструкції працівниками та посадовими особами винні особи можуть бути притягнені до дисциплінарної відповідальності.

Виконувач обов’язків керівника
апарату військової адміністрації **Володимир КОЦЮК**

Оксана Волох