БЕРЕСТИНСЬКА РАЙОННА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
ХАРКІВСЬКОЇ ОБЛАСТІ

Р О З П О Р Я Д Ж Е Н Н Я

12 березня 2025 року **Берестин** № 39

Про політику інформаційної безпеки у Берестинській районній державній (військовій) адміністрації

Відповідно до законів України «Про правовий режим воєнного стану», «Про інформацію», «Про основні засади забезпечення кібербезпеки України», Указу Президента України від 24 лютого 2022 року №68/2022 «Про утворення військових адміністрацій», Указу Президента України від 24 лютого 2022 року «Про введення воєнного стану в Україні» (зі змінами), Указу Президента України від 26 серпня 2021 року №447/2021 «Про Стратегію кібербезпеки», наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03 липня 2023 року № 570 «Про завтердження Методичних рекомендаціях щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», з метою підвищення рівня кіберзахисту районної військової адміністрації **зобов'язую:**

1. Визначити відділ організаційної роботи апарату районної державної (військової) адміністрації відповідальним за інформаційну безпеку у Берестинській районній державній (військовій) адміністрації.

2. Затвердити політику інформаційної безпеки у Берестинській районній державній (військовій) адміністрації, що додається.

3. Відділу організаційної роботи апарату районної державної (військової) адміністрації ознайомити усіх працівників структурних підрозділів районної державної (військової) адміністрації із політикою інформаційної безпеки у Берестинській районній державній (військовій) адміністрації та забезпечувати дотримання встановлених вимог відповідно до пункту 2 цього розпорядження.

4. Координацію роботи щодо виконанням розпорядження покласти на керівника апарату районної державної (військової) адміністрації Людмилу ЧИСТІКОВУ, контроль – на першого заступника начальника районної військової адміністрації Наталію ОСАДЧУ.

Начальник районної військової адміністрації **Віктор ВОЙТЕНКО**

ЗАТВЕРДЖЕНО
розпорядження начальника районної
військової адміністрації
12 березня 2021 року № 39

Політика інформаційної безпеки
у Берестинській районній державній (військовій) адміністрації

1. Загальні положення

1.1. Політика інформаційної безпеки у Берестинській районній державній (військовій) адміністрації (далі – Політика) визначає основні принципи, підходи та заходи щодо забезпечення захисту інформації та інформаційних ресурсів від несанкціонованого доступу, втрати, пошкодження або викрадення, а також позицію керівництва Берестинської районної державної (військової) адміністрації в питаннях інформаційної безпеки.

Політика є основою для захисту інформаційних активів, забезпечення їх конфіденційності, цілісності, доступності та спостережності.

1.2. Дія цього документа поширюється на всіх працівників районної державної (військової) адміністрації, а також на осіб, які мають доступ до інформації, що обробляється в районній державній (військовій) адміністрації. Дотримання цієї Політики є обов'язковим.

1.3. Політика розроблена відповідно до вимог законодавства України у сфері інформаційної безпеки та кіберзахисту, враховуючи відсутність Інформаційно-комунікаційної системи (ІКС) в районній державній (військовій) адміністрації.

2. Основні принципи інформаційної безпеки

2.1. Конфіденційність – забезпечення доступу до інформації лише уповноваженим особам.

2.2. Цілісність – захист даних від несанкціонованої модифікації або знищення.

2.3. Доступність – гарантування своєчасного доступу до інформаційних ресурсів уповноваженим особам.

2.4. Відповідальність – кожен співробітник несе відповідальність за дотримання вимог інформаційної безпеки.

3. Мета та цілі політики інформаційної безпеки

3.1. Основною метою Політики є захист суб'єктів інформаційних відносин районної державної (військової) адміністрації від можливої матеріальної, фізичної, моральної або іншої шкоди шляхом випадкового або навмисного впливу на інформацію, її носії, процеси обробки та передачі, а також мінімізація рівня операційних та інших ризиків.

3.2. Цілі заходів та вимоги інформаційної безпеки визначають застосовність сервісів безпеки за принципами: доступності, цілісності, конфіденційності, спостережності – для захисту інформації, ресурсів ІТ-інфраструктури та процесів діяльності районної державної (військової) адміністрації.

Джерелами для формування цілей заходів та вимог інформаційної безпеки можуть бути зовнішні та внутрішні фактори, що визначають діяльність районної державної (військової) адміністрації, а саме: закони України, стандарти інформаційної безпеки, угоди з третіми сторонами, внутрішні нормативні документи, що регламентують принципи обміну та обробки інформації відповідно до її потреб.

3.3. Основні завдання Політики:

1) своєчасне виявлення, оцінка та прогнозування джерел загроз безпеці, причин та умов, що сприяють нанесенню шкоди зацікавленим суб'єктам інформаційних відносин, порушенню нормального функціонування районної державної (військової) адміністрації;

2) забезпечення дотримання процесу оперативного реагування на інциденти інформаційної безпеки;

3) мінімізація та локалізація шкоди від неправомірних дій персоналу або третіх осіб, пом'якшення негативного впливу та ліквідація наслідків порушення інформаційної безпеки;

4) обмеження доступу користувачів до інформації, апаратних, програмних та інших ресурсів районної державної (військової) адміністрації за принципом «службової необхідності» (можливість доступу тільки до тих ресурсів і виконання операцій, які необхідні конкретним користувачам для виконання своїх службових обов'язків), захист від несанкціонованого доступу;

5) забезпечення авторизації та аутентифікації користувачів, які беруть участь в інформаційному обміні (підтвердження автентичності відправника та отримувача інформації);

6) захист від несанкціонованої модифікації та контроль цілісності програмного забезпечення, що використовується в інформаційному середовищі районної державної (військової) адміністрації, а також захист систем від впровадження несанкціонованих програм, в тому числі шкідливих програм;

7) захист інформації з обмеженим доступом від витоку соціальними або технічними каналами під час її обробки, зберігання та передачі каналами зв'язку,

а також захист від несанкціонованого розголошення або модифікації такої інформації.

4. Об'єкти та суб'єкти інформаційної безпеки

4.1. Об'єкти інформаційної безпеки. Основними об'єктами інформаційної безпеки у районній державній (військовій) адміністрації є:

інформаційні ресурси, у тому числі відкрита (загальнодоступна) інформація, що представлена у вигляді документів та масивів інформації, незалежно від форми та виду її представлення;

інфраструктура, що включає системи обробки та аналізу інформації, технічні та програмні засоби її обробки, передачі та відображення, у тому числі канали інформаційного обміну та телекомунікації, системи та засоби захисту інформації, об'єкти та приміщення, в яких розміщені чутливі компоненти автоматизованої системи.

4.2. Суб'єкти інформаційної безпеки. Суб'єктами забезпечення інформаційної безпеки у районній державній (військовій) адміністрації є:

Берестинська районна державна (військова) адміністрація, як власник інформаційних ресурсів;

голова (начальник) Берестинської районної державної (військової) адміністрації;

відділ організаційної роботи апарату районної державної (військової) адміністрації, який визначений відповідальним за інформаційну безпеку у районній державній (військовій) адміністрації;

керівники структурних підрозділів районної державної (військової) адміністрації;

треті сторони, які залучаються для надання послуг у Берестинській районній державній (військовій) адміністрації.

5. Розподіл обов'язків у сфері інформаційної безпеки

5.1. Ефективна підтримка політики інформаційної безпеки у районній державній (військовій) адміністрації вимагає активної підтримки та постійного залучення співробітників на всіх рівнях управління. Кожен співробітник повинен нести відповідальність за виконання вимог даної Політики у межах своїх посадових обов'язків.

5.2. Районна державна (військова) адміністрація повинна забезпечувати виконання вимог для підтримки інформаційної безпеки в належному стані, що відповідає вимогам чинного законодавства, нормативно-правовим актам, міжнародним стандартам, а також контрактним зобов'язанням:

розробку та перегляд політики відповідно до загального напрямку діяльності районної державної (військової) адміністрації в сфері інформаційної безпеки;

ідентифікацію активів, призначення відповідальних за їх безпеку;

використання рішень для шифрування для захисту конфіденційності, цілісності, доступності та/або спостережності інформації;

запобігання несанкціонованому доступу до приміщень, а також захист обладнання та устаткування від компрометації внаслідок втручання людини або природних факторів;

захист ІТ-систем, включаючи операційні системи та програмне забезпечення, від втрати даних;

захист мережевої інфраструктури та сервісів, а також інформації, що передається через них;

врахування інформаційної безпеки при придбанні нових інформаційних систем або модернізації існуючих;

належне інформування та обробку подій та інцидентів, пов'язаних з безпекою, з метою їх своєчасного вирішення;

безперервність захисту Інформації та доступність інформаційних систем під час збоїв;

запобігання порушенням правових, законодавчих, регуляторних та договірних норм;

систематичне навчання співробітників районної державної (військової) адміністрації з питань інформаційної безпеки.

5.2. Голова (начальник) районної державної (військової) адміністрації несе відповідальність за:

затвердження нормативних документів, програми навчання та підвищення обізнаності персоналу в сфері інформаційної безпеки;

призначення відповідального відділу за перегляд Політики;

забезпечення необхідних і достатніх ресурсів (включаючи персонал і фінансування) для впровадження та підтримки інформаційної безпеки.

5.3. Відділ організаційної роботи апарату районної державної (військової) адміністрації несе відповідальність за:

інвентаризацію та класифікацію інформаційних активів;

розробку та впровадження організаційних заходів безпеки;

створення принципів та цілей інформаційної безпеки;

розслідування інцидентів інформаційної безпеки разом з відповідною третьою стороною (за необхідністю);

моніторинг подій інформаційної безпеки;

налаштування робочих пристроїв відповідно до вимог безпеки.

5.4. Всі працівники районної державної (військової) адміністрації несуть відповідальність за:

безпеку інформації районної державної (військової) адміністрації;

участь в управлінні інцидентами інформаційної безпеки;

використання адекватної інформації відповідно до цілей, для яких вона обробляється;

нерозголошення або невикористання інформації з обмеженим доступом на власну користь або користь інших осіб.

6. Захист інформаційних ресурсів

6.1. Усі документи та дані, що обробляються в районній державній (військовій) адміністрації, мають зберігатися у відповідності до вимог інформаційної безпеки.

6.2. Доступ до інформаційних ресурсів надається лише на основі необхідності виконання службових обов'язків.

6.3. Використання особистих пристроїв для роботи з конфіденційною інформацією заборонено.

6.4. Регулярне здійснення резервного копіювання важливих документів для запобігання їх втраті у випадку інцидентів.

7. Захист від кіберзагроз

7.1. Запровадження антивірусного захисту та заходів щодо запобігання витоку інформації.

7.2. Забороняється встановлення несанкціонованого програмного забезпечення на службові пристрої.

7.3. Забезпечення всіх електронних пристроїв захищеними паролями.

7.4. Запобігання фішинговим атакам та іншим методам соціальної інженерії.

8. Управління інцидентами інформаційної безпеки

8.1. Негайне інформування відповідальних осіб у разі виявлення підозрілих дій або кібератак згідно Порядку реагування на кібератаки та кіберінциденти у районній державній (військовій) адміністрації.

8.2. Реєстрація, аналіз та документування для подальшого вдосконалення заходів безпеки всіх інцидентів.

8.3. Вжиття оперативних заходів для усунення загроз, а також проведення розслідування причин інциденту.

9. Навчання та підвищення обізнаності

9.1. Обов'язкове проходження навчання з інформаційної безпеки співробітниками районної державної (військової).

9.2. Участь у тренінгах та проходження тестувань з визначення знань з безпечного використання інформаційних ресурсів.

10. Відповідальність за порушення політики

10.1. Недотримання вимог цієї політики може призвести до дисциплінарної відповідальності відповідно до чинного законодавства.

10.2. У разі умисного розголошення конфіденційної інформації або спричинення шкоди інформаційним ресурсам винні особи притягуються до відповідальності згідно вимог чинного законодавства.

11. Заключні положення

11.1. Ця Політика є легкодоступною для персоналу та третіх сторін (за необхідності) для використання та є обов'язковою для виконання всіма співробітниками районної державної (військової) адміністрації.

11.2. Політика переглядається та оновлюється у разі змін законодавства або виникнення нових загроз інформаційній безпеці.

Керівник апарату районної
військової адміністрації **Людмила ЧИСТІКОВА**

Віра Педаш