БІЛГОРОД-ДНІСТРОВСЬКА МІСЬКА РАДА

Р О З П О Р Я Д Ж Е Н Н Я

МІСЬКОГО ГОЛОВИ

від _____ 20___ р. № _____

Про систему захисту інформації
в Білгород-Дністровській
міській раді

З метою забезпечення надійного захисту інформації, що обробляється в інформаційно-комунікаційній системі Білгород-Дністровської міської ради, від несанкціонованого доступу, знищення, модифікації, спотворення та інших неправомірних дій, відповідно до законів України «Про місцеве самоврядування», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про інформацію», «Про державну таємницю» та нормативних документах системи технічного захисту інформації (НД ТЗІ), затверджені Держспецзв'язку України, , керуючись частиною другою, пунктом 20 частини четвертої статті 42, частиною восьмою статті 59 Закону України «Про місцеве самоврядування в Україні»,

ЗОБОВ'ЯЗУЮ:

1. Затвердити Положення про систему захисту інформації в Білгород-Дністровській міській раді (далі – Положення), що додається.
2. Затвердити Інструкцію користувача інформаційно-комунікаційної системи в Білгород-Дністровській міській раді (далі – Інструкція), що додається.
3. Відділу з питань цифрового розвитку та інновацій, цифрових трансформацій і цифровізації Білгород-Дністровської міської ради ознайомити всіх працівників апарату Білгород-Дністровської міської ради та виконавчих органів міської ради з Положенням та Інструкцією.
4. Відповідальність за організацію виконання даного розпорядження покласти на головного спеціаліста – адміністратора безпеки відділу з питань цифрового розвитку та інновацій, цифрових трансформацій і цифровізації Олександра МЕЛЬНИКОВА.
5. Контроль за виконанням цього розпорядження покласти на заступника міського голови Андрія КРИШТОПОВА.

Секретар міської ради Олександр СКАЛОЗУБ

СЕД АСКОД - ВИКОНАВЧИЙ КОМІТЕТ БІЛГОРОД-ДНІСТРОВСЬКОЇ МІСЬКОЇ РАДИ
№ документа: 174
Дата реєстрації: 04.12.2025
Сертифікат: 6FA97849F1B2570D04000000F15001005B490800
Дійсний з: 21.08.2025 13:09:22
Дійсний до: 21.08.2026 13:09:22
Підписувач: Скалозуб Олександр Васильович
Мітка часу: 03.12.2025 16:57:21

ЗАТВЕРДЖЕНО
Розпорядження міського голови
Білгород-Дністровської ради
_____№_____

Положення про систему захисту інформації
в Білгород-Дністровській міській раді

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. Положення про систему захисту інформації в інформаційно-комунікаційних системах (далі – Положення) є основним організаційно-розпорядчим документом, що встановлює єдині вимоги до захисту інформації з обмеженим доступом, яка обробляється в інформаційно-комунікаційних системах (далі – ІКС) Білгород-Дністровської міської ради (далі – Білгород-Дністровська МР).

2. Це Положення розроблено відповідно до чинного законодавства України у сфері захисту інформації.

3. Вимоги цього Положення поширюються на всіх працівників Білгород-Дністровської МР та підвідомчих установ, які використовують ІКС для обробки інформації з обмеженим доступом.

4. Зміни та доповнення до цього Положення затверджуються розпорядженням голови Білгород-Дністровської МР.

ІІ. НОРМАТИВНІ ПОСИЛАННЯ

Це Положення розроблено з урахуванням вимог таких нормативно-правових актів:

Закон України «Про захист інформації в інформаційно-комунікаційних системах»;

Закон України «Про інформацію»;

Закон України «Про державну таємницю»;

Закон України «Про захист персональних даних»;

Нормативні документи системи технічного захисту інформації (НД ТЗІ), затверджені Держспецзв’язку України.

ІІІ. МЕТА ТА ЗАВДАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1. Метою системи захисту інформації (далі - СЗІ) є забезпечення надійного захисту інформації, що обробляється в ІКС Білгород-Дністровської МР, від несанкціонованого доступу, знищення, модифікації, спотворення та інших неправомірних дій.

2. Основними завданнями СЗІ є:

забезпечення конфіденційності інформації – запобігання несанкціонованому ознайомленню з інформацією;

забезпечення цілісності інформації – запобігання несанкціонованій модифікації інформації;

забезпечення доступності інформації – запобігання блокуванню доступу до інформації;

Запобігання інцидентам інформаційної безпеки та забезпечення безперервності роботи ІКС.

ІV. СКЛАД СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Система захисту інформації є комплексною і складається з:

організаційних заходів: розробка та впровадження внутрішніх нормативних документів, інструктаж та навчання персоналу, контроль дотримання вимог безпеки;

технічних (інженерних) засобів: фізичний захист об'єктів (СКУД, сигналізація, відеоспостереження), захист комунікаційних ліній;

програмно-апаратних засобів: використання антивірусного програмного забезпечення, міжмережевих екранів, засобів криптографічного захисту інформації (КЗІ) та засобів захисту від несанкціонованого доступу (ЗНСД).

V. ПОРЯДОК ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1. Управління доступом: доступ користувачів до ресурсів ІКС надається лише після їх офіційного допуску та ознайомлення з відповідними інструкціями. Дозволи на доступ надаються згідно з посадовими обов'язками.

2. Правила роботи з паролями: кожен користувач зобов'язаний використовувати складні та унікальні паролі, які періодично змінюються. Забороняється розголошувати або записувати паролі на матеріальних носіях.

3. Робота з інформацією: користувачі повинні використовувати лише не заборонене програмне забезпечення. Забороняється завантажувати та встановлювати будь-які програми без дозволу системного адміністратора.

4. Моніторинг та аудит: усі події, пов'язані з доступом до інформації (успішні/невдалі спроби входу, доступ до файлів), повинні реєструватися та періодично аналізуватися відповідальним за безпеку.

VI. ВІДПОВІДАЛЬНІСТЬ

1. Відповідальність за забезпечення захисту інформації в системі покладається на відділ з питань цифрового розвитку та інновацій, цифрових трансформацій і цифровізації міської ради.

2. Кожен користувач ІКС несе персональну відповідальність за дотримання вимог цього Положення та Інструкції користувача ІКС, з якою він ознайомлений під підпис.

VII. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

1. Експлуатація ІКС та обробка в ній інформації може здійснюватися лише після успішного проведення атестації комплексної системи захисту інформації.

Це Положення вступає в силу з моменту його затвердження.

_____

ЗАТВЕРДЖЕНО
Розпорядження міського голови
Білгород-Дністровської ради
_____№_____

Інструкція користувача інформаційно-комунікаційної системи в Білгород-Дністровській міській раді

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця інструкція визначає правила та вимоги щодо роботи з інформаційно-комунікаційними системами (ІКС) та інформацією з обмеженим доступом.

1.2. Кожен користувач несе персональну відповідальність за дотримання вимог цієї інструкції. Порушення може призвести до дисциплінарної, адміністративної або кримінальної відповідальності.

1.3. Користувач має право доступу лише до тих ресурсів та даних, які необхідні для виконання його посадових обов'язків.

2. ПРАВИЛА РОБОТИ З ОБЛІКОВИМИ ЗАПИСАМИ ТА ПАРОЛЯМИ

2.1. Облікові записи:

кожен користувач повинен мати унікальний обліковий запис;

забороняється передавати свій обліковий запис та пароль іншим особам;

забороняється використовувати чужі облікові записи.

2.2. Паролі:

пароль повинен бути складним, містити не менше 8 символів та включати великі та малі літери, цифри та спеціальні символи;

пароль необхідно змінювати не рідше одного разу на 90 днів;

забороняється зберігати паролі на паперових носіях або в незахищених електронних файлах.

3. ПРАВИЛА РОБОТИ З ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

3.1. Електронна пошта:

не відкривайте вкладення та не переходьте за посиланнями у листах від невідомих відправників;

перевіряйте адреси відправників на наявність підозрілих символів або помилок;

забороняється передавати чи надсилати службову інформацію через будь-які електронні поштові сервіси та адреси, що не належать до офіційних поштових доменів державних органів України (@*.gov.ua).

3.2. Знімні носії інформації:

перед використанням будь-якого флеш-накопичувача або іншого знімного носія, його необхідно перевірити антивірусною програмою;

забороняється використовувати особисті флеш-накопичувачі для роботи з конфіденційною інформацією;

носії інформації з обмеженим доступом повинні зберігатися у спеціально відведених місцях.

3.3. Робоче місце:

виконуйте політику «чистого столу», не залишайте на робочому місці документи, що містять конфіденційну інформацію.

виконуйте політику «чистого екрану», блокуйте свій комп'ютер, коли відходите від нього (комбінація клавіш `Windows + L`).

4. РЕАГУВАННЯ НА ІНЦИДЕНТИ

4.1. У разі виявлення підозрілої активності, вірусу, несанкціонованого доступу або будь-якого іншого інциденту, користувач зобов'язаний негайно повідомити про це адміністратора безпеки.

4.2. Ознаки інциденту:

підозрілі повідомлення або спливаючі вікна;

незвичайна поведінка програмного забезпечення;

відсутність доступу до даних або їх спотворення;

спроби несанкціонованого доступу до вашого облікового запису.

4.3. У разі підозри на компрометацію облікового запису, негайно змініть пароль.