проєкт

РОГАТИНСЬКА МІСЬКА РАДА
ІВАНО-ФРАНКІВСЬКА ОБЛАСТЬ
ВИКОНАВЧИЙ КОМІТЕТ

Р І Ш Е Н Н Я

від 25 листопада 2025 року №
м.Рогатин

Про затвердження
Політики інформаційної безпеки
та Плану реагування на кіберінциденти

З метою виконання вимог Законів України «Про інформацію», «Про захист інформації в інформаційнокомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», Указу Президента України від 26.08.2021 №447/2021 «Про Стратегію кібербезпеки України», наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту», відповідно до статтей 38,59 Закону України «Про місцеве самоврядування в Україні», виконавчий комітет міської ради ВИРІШИВ:

1.Затвердити Політику інформаційної безпеки виконавчого комітету Рогатинської міської ради (додаток 1).

2. Затвердити План реагування на кіберінциденти (додаток 2).

3.Начальнику відділу забезпечення роботи інформаційно-комунікаційних систем (Р.Гаврилюку):

3.1. в термін до 30.12.2025р. забезпечити підключення до платформи обміну індикаторами компрометації MISP CERT-UA та адаптованого програмного продукту MISP-UA;

3.2.провести оцінку та визначення поточного профілю кіберзахисту виконавчого комітету Рогатинської міської ради відповідно до Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту, затверджених наказом Адміністрації Держспецзв'язку від 30.01.2025 № 54 до 30.12.2025р.;

4. Керівникам комунальних підприємств, установ та закладів Рогатинської міської ради забезпечити виконання вимог цього рішення.

5. Відповідальним особам за інформаційну безпеку ознайомити працівників виконавчих органів міської ради з «Політикою інформаційної безпеки Виконавчого комітету Рогатинської міської ради» та «Планом реагування на кіберінциденти».

6. Контроль за виконанням даного рішення покласти на керуючого справами виконавчого комітету Олена ВОВКУНА.

Міський голова Сергій НАСАЛИК

Керуючий справами
виконавчого комітету Олег ВОВКУН

Додаток 1
до рішення виконавчого комітет
Рогатинської міської ради
від 25 листопада 2025 року №____

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
виконавчого комітету
Рогатинської міської ради

Зміст

1. Загальні положення

Політика інформаційної безпеки (далі – Політика) визначає загальні вимоги до інформаційної безпеки у виконавчих органах, підприємствах, установах та закладах, що перебувають у віданні Рогатинської міської ради (далі – Суб'єкти), основні принципи, цілі та завдання управління інформаційною безпекою у системі органів місцевого самоврядування Рогатинської міської територіальної громади.

Дана Політика є обов'язковим документом для ознайомлення при прийомі на роботу працівників, які працюватимуть з електронними засобами на яких створюється офіційна інформація та персональні дані.

Ця Політика є офіційно прийнятою виконавчим комітетом Рогатинської міської ради способом впливу на проблеми забезпечення інформаційної безпеки, встановлює принципи побудови процесів управління інформаційною безпекою на основі систематизованої розробки та впровадження політик, положень, регламентів, стандартів, інструкцій та інших нормативних документів у сфері інформаційної безпеки.

Метою даної Політики є:

- Забезпечення захисту інформаційних ресурсів Суб'єктів від зовнішніх і внутрішніх загроз;
- Безперервність роботи всіх служб і сервісів Суб'єктів;
- Мінімізація ризиків операційної діяльності Суб'єктів;
- Створення позитивної репутації ТГ при взаємодії з третіми особами;
- Відповідність законодавству України рівня інформаційної безпеки та захисту персональних даних.

Дана Політика поширюється на всі процеси діяльності Суб'єктів та є обов'язковою для виконання всіма їх співробітниками. Порушення вимог Політики тягне за собою дисциплінарну відповідальність та іншу відповідальність згідно з чинним законодавством України.

2. Терміни та визначення

Власник інформаційного активу (ІА) – співробітник Суб'єкта, який несе відповідальність за: забезпечення належної класифікації інформації та активів, пов'язаних із засобами обробки інформації; визначення та періодичний перегляд обмежень доступу і класифікацій; управління конкретними ризиками, пов'язаними з активом, і визначення пов'язаних потреб в безпеці.

Вплив – величина збитку, який можна очікувати в результаті наслідків несанкціонованого розкриття інформації, несанкціонованої зміни інформації, несанкціонованого знищення інформації або втрати інформації або порушення доступності інформаційної системи.

Доступність – властивість інформації, яка полягає в тому, щоб бути доступною та використовуватися на вимогу користувача і/або процесу.

Загроза – можлива небезпека, яка може використовувати уразливість в інформаційній системі для порушення цілісності, конфіденційності, доступності системи.

Інформаційна безпека (ІБ) – це практика забезпечення захисту інформаційних активів від загроз, які можуть на них вплинути. Вона включає в себе вичерпний набір засобів управління, які охоплюють різні фактори (людські, фізичні, екологічні та технічні) протягом життєвого циклу інформаційних і технологічних активів, включаючи розробку, створення і впровадження нових систем, підтримка даних і систем, моніторинг використання таких активів, виявлення та реагування на потенційні загрози, дотримання чинних законів і положень про кібербезпеку і конфіденційність, а також виведення з експлуатації ІТ-систем і знищення даних.

Інформаційна система – комп'ютерні системи, програмне забезпечення, телекомунікаційне і периферійне устаткування.

Інформаційний актив (ІА) – обладнання, програмне забезпечення, дані, а також співробітники, які беруть участь в процесах діяльності ТГ, які визначені і управляються як єдине ціле, щоб його можна було зрозуміти, спільно використовувати, захищати та ефективно керувати. Інформаційні активи мають керовану цінність, ризики, контент і життєві цикли.

Інцидент – це подія, яка не є частиною звичайних операцій і порушує робочі процеси. Інцидент може включати відмову функції або послуги, які повинні були бути надані, або будь-які інші типи збою операції.

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Користувач – особа або Суб'єкти, які взаємодіють з інформаційними системами.

Оцінка ризиків – процес виявлення, визначення пріоритетів та аналіз ризиків. Процес включає визначення ступеня, в якому несприятливі обставини або події

можуть вплинути на Суб'єкта. Даний процес використовує результати оцінок загроз і вразливостей для виявлення ризиків для діяльності Суб'єкта і оцінює ці ризики, з точки зору ймовірності виникнення і впливу. Результатом оцінки ризику є список передбачуваних потенційних впливів і явних вразливостей. Оцінка ризиків є частиною процесу управління ризиками.

Політика інформаційної безпеки – набір задокументованих управлінських рішень, створений для захисту інформації Суб'єкта та пов'язаних з нею ресурсів.

Ризик – ймовірність впливу на діяльність Суб'єкта (включаючи місію, функції, імідж, репутацію), її активи (ресурси) і співробітників в результаті експлуатації вразливостей інформаційної системи і залежно від потенційного впливу, реалізація загрози і ймовірність її реалізації.

Уразливість – недолік в інформаційній системі, який може бути використаний суб'єктом загрози (наприклад, зловмисником) для виконання несанкціонованих дій в системі і порушення цілісності, конфіденційності, доступності або спостережливості.

Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Шифрування – процес перетворення відкритого тексту в зашифрований з метою безпеки або конфіденційності.

Шкідливе ПЗ – програмне забезпечення, яке вживлюється в систему, як правило, таємно, з метою порушення конфіденційності, цілісності та/або доступності даних, додатків або операційної системи користувача або іншим чином шкодити або заважати роботі користувача.

SMTPS – Simple Mail Transfer Protocol Secure.

3.Політика інформаційної безпеки

3.1. Управління інформаційною безпекою

Для забезпечення ІБ, необхідно слідувати формальним загальним правилам та процедурам наведеним далі, що покривають відповідне використання ІА Суб'єкта. Співробітники Суб'єкта та відповідні треті сторони (які мають доступ до інформації та/або ресурсів ТГ) повинні бути проінформовані про необхідність дотримання цієї Політики.

Для забезпечення постійної придатності, адекватності та ефективності ця Політика повинна переглядатися Відповідальною особою за інформаційну безпеку через заплановані проміжки часу – щонайменше раз в рік, якщо впроваджуються суттєві зміни або за рішенням Керівництва Суб'єкта.

Суттєвими змінами можна вважати:

- Зміни в процесах діяльності Суб'єкта;
- Зміни в організаційній структурі тощо.

Відповідно до сфери діяльності Суб'єкта необхідно також враховувати наступні моменти:

- Законодавство, що регулює сферу діяльності Суб'єкта та договірні зобов'язання;
- Відповідальність за порушення Політики;
- Обов'язки Керівництва Суб'єкта та інших осіб щодо безпеки систем та інформації Суб'єкта.

3.2. Розподіл обов'язків з інформаційної безпеки

Загальна відповідальність за ІБ Суб'єкта покладається на відділ забезпечення роботи інформаційно-комунікаційних систем.

Відділ відповідальний за:

- Визначення критичних операційних процесів для діяльності Суб'єкта;
- Прийняття рішень щодо розвитку ІБ Суб'єкта;
- Затвердження та поширення правил і вимог ІБ в ТГ;
- Затвердження відповідальності за порушення правил та вимог ІБ;
- Функцію перевірки та контролю виконання в ТГ правил та вимог ІБ.

Додатково відповідальні та їх обов'язки описані нижче.

3.3. Безпека людських ресурсів

Перевірка кандидатів перед працевлаштуванням, співробітників чи третіх осіб повинна чітко враховувати чутливість інформації, до якої кандидати отримають доступ, та передбачувані ризики при визначенні характеру та строків цих перевірок.

Призначення на посади та звільнення з посад повинно виконуватися відповідно до державних нормативно-правових актів.

Кожен співробітник Суб'єкта та третьої особи, якому надано доступ до систем та/або даних Суб'єкта, несе відповідальність за безпечне використання систем і даних для цілей діяльності ТГ та дотримання її політик.

Співробітники та треті особи несуть відповідальність за повідомлення Керівнику про будь-які сумніви щодо ефективності процесів безпеки, про будь- яку подію чи інцидент щодо несанкціонованого або неправильного використання активів Суб'єкта.

Обов'язок відповідальних осіб за ІБ ТГ вимагати від всіх співробітників та третіх осіб дотримання вимог ІБ ТГ, відповідно до встановлених політик та процесів, а також контролювати процес їх дотримання.

Припинення трудової діяльності здійснюється згідно з чинним трудовим законодавством України.

3.4. Навчання та обізнаність

Всі співробітники, які є користувачами внутрішньої мережі зобов'язані дотримуватись внутрішніх вимог щодо роботи з інформаційними активами Суб'єкта та нести персональну відповідальність за їх дотримання.

Усі співробітники та відповідні треті особи повинні проходити відповідну підготовку з підвищення обізнаності та регулярно отримувати інформацію про

оновлення організаційних політик та процедур відповідно до їх робочих функцій.
Усі співробітники повинні підтримувати базовий рівень розуміння питань ІБ, таких як загальні зобов'язання згідно з різними політиками, стандартами, процедурами, керівними принципами, законами, нормативними актами, контрактними умовами, а також загальноприйнятими стандартами етики та прийнятної поведінки.
Додаткове навчання проводиться для співробітників, які мають конкретні зобов'язання щодо захисту інформації та кому не вистачає базової обізнаності щодо ІБ в рамках робочого процесу, наприклад, адміністраторам систем, відповідальним за ІБ. Такі вимоги до навчання повинні бути визначені в посадових обов'язках та особистих планах навчання співробітників.

3.5. Фізична безпека

Засоби обробки інформації повинні розміщуватися в захищених зонах, фізично захищених від несанкціонованого доступу, пошкодження та втручання чи зміни певних периметрів безпеки. Для виявлення або запобігання несанкціонованого доступу та захисту ІА, особливо критичних і чутливих, повинні застосовуються багаторівневі внутрішні та зовнішні засоби контролю від примусових або прихованих атак.

3.6. Класифікація та управління інформацією

Інформацію слід класифікувати, визначати та оцінювати ризики відповідно до її конфіденційності, цілісності, доступності та спостережливості, незалежно від носія, на якому вона зберігається і/або обробляється. Чутлива інформація повинна визначатися відповідно до її конфіденційності, цілісності, доступності та спостережливості. Вся інформація, окрім публічної, має визначатися як чутлива.
Незалежно від рівня конфіденційності, вся інформація Суб'єкта повинна використовуватися належним чином та тільки для дозволених цілей.
Розкриття інформації з обмеженим доступом може здійснюватися лише у законний спосіб зацікавленим особам органів влади, а також фізичним та юридичним особам за згодою Суб'єкта, з дотриманням вимог чинного законодавства України та вимог відповідних Договорів.

3.7. Обробка, передача та зберігання даних

Чутливі дані повинні збиратися та зберігатися лише в системах, де є обґрунтована ділова чи технічна потреба. Чутливі виробничі дані повинні бути захищені при зберіганні і/або використанні у системах, і надійно видалятись, коли вони більше не потрібні.
Чутливі дані ніколи не повинні збиратися або використовуватися для цілей, відмінних від тих, для яких дані були зібрані спочатку. Усі параметри збереження даних (періоди, цілі тощо) повинні бути законними та відповідати місцевому та міжнародному законодавству та нормам щодо захисту даних.

3.8. Використання особистих пристроїв

Суб'єкт може дозволяти співробітникам та іншим авторизованим користувачам своїх систем, послуг та ресурсів використовувати власні пристрої для виконання посадових обов'язків та завдань, які необхідні для забезпечення її безперервної діяльності.

Суб'єкт повинен розробити та встановити вимоги ІБ щодо використання власних робочих пристроїв та довести їх до відома усіх співробітників та відповідних третіх осіб. Особисту відповідальність має нести кожен співробітник та третя особа, що використовує персональний пристрій для доступу до систем, послуг та ресурсів Суб'єкта, щоб забезпечити відповідне використання всіх протоколів безпеки та усіх заходів безпеки.

Кожен пристрій, який використовується для виконання посадових обов'язків та завдань, які необхідні для забезпечення безперервної діяльності Суб'єкта, тобто для доступу до внутрішньої інформації, повинен використовуватися відповідально та лише в службових цілях.

3.9. Доступ до мережі та мережевих сервісів

Користувачам повинен надаватися доступ до мережі та мережевих послуг, у разі необхідності такого доступу.

Повинен бути встановлений контроль за переглядом та управлінням доступу, включаючи контроль та впровадження наступних засобів та інструментів:

- Перелік мереж та мережевих послуг з дозволеним доступом;
- Процедури визначення необхідного доступу та відповідних користувачів;
- Інструменти для управління мережевими з'єднаннями та послугами;
- Засоби та інструменти моніторингу використання мережевих послуг.

3.10. Парольна політика

Відповідно до Парольної політики, для забезпечення надійного захисту інформаційних систем паролем, мають бути встановлені наступні параметри:

- Мінімальна довжина: 8-12 символів;
- Повинен містити символи верхнього та нижнього регістру, числа, а також неалфавітні символи;
- Не використовувати будь-які персональні дані;
- Не містить у собі загальновживані слова;
- Мінімальний термін дії пароля: 1 день;
- Максимальний термін дії пароля: 30-90 днів;
- Зберігати паролі за допомогою оборотного шифрування: ні;
- Сповіщення про зміну: за 7 днів до закінчення терміну дії;
- Історія паролів: 10 останніх використаних паролів;
- Поріг блокування облікового запису: 5 послідовних невдалих спроб введення;

- Скинути лічильник блокування облікового запису через: 15 хвилин;
- Безпечне зберігання паролів: паролі не слід зберігати або передавати у відкритому тексті.

3.11. Використання електронної пошти

Доступ до електронної пошти надається співробітникам Суб'єкта для виконання своїх службових обов'язків. Використання електронної пошти співробітниками Суб'єкта в особистих або інших цілях, не пов'язаних з діяльністю Суб'єкта, заборонено.

В діяльності Суб'єкта заборонено:

- Надсилати повідомлення, що містять чутливу інформацію, а також дані, що містять чутливу інформацію не для виконання своїх службових обов'язків. Забороняється надсилати по електронній пошті логіни, паролі та іншу чутливу інформацію;
- Використовувати електронну пошту для особистих цілей;
- Використовувати електронну адресу для підписки на маркетингові електронні листи без попереднього узгодження з Відповідальною особою за ІБ;
- Відкривати будь-яке вкладення, посилання чи додаток до електронної пошти, де співробітник не має ґрунтовних підстав вважати, що інформація, до якої очікується доступ, надійшла з надійного джерела;
- Надсилати по електронній пошті матеріали, що містять шкідливе програмне забезпечення чи інші програми, призначені для порушення, знищення або обмеження функціональних можливостей будь-якого комп'ютерного чи телекомунікаційного обладнання чи інформаційних систем та послуг;
- Надсилати електронною поштою програми, які забезпечують несанкціонований доступ;
- Розповсюджувати за допомогою електронної пошти матеріали, які захищені авторським правом і зачіпають будь-який патент, торгову марку, комерційну таємницю, авторські права або будь-які інші права власності. та/або авторські права або пов'язані з ними права третіх сторін;
- Поширювати через електронну пошту інформацію, заборонену міжнародним та українським законодавством, включаючи матеріали, що є шкідливими, загрозливими, нецензурними, а також інформацію, що порушує честь та гідність інших осіб. Також забороняється надсилати матеріали, що розпалюють національну ворожнечу, підбурюють до насильства, закликають до незаконних дій, включаючи матеріали, що містять інструкції щодо використання вибухових речовин, зброї тощо.

Доступ колишнього співробітника до облікових записів електронної пошти Суб'єкта повинен бути негайно відключений та деактивований.

3.12. Безпека мережі

Наступні вимоги обов'язкові до виконання:

- Вимоги до конфігурації безпеки повинні бути визначені для всього мережевого обладнання;
- Вимоги до контролю аутентифікації та доступу повинні бути визначені та повинні бути впроваджені;
- Вимоги до систем та механізмів моніторингу безпеки мережі повинні бути визначені, впровадженні, необхідним чином управлятися;
- Усі оновлення повинні вчасно встановлюватись;
- Зміни можуть бути внесені лише адміністратором систем або відповідним авторизованим користувачем;
- Процес резервного копіювання мережевих пристроїв (наприклад, системного програмного забезпечення, даних конфігурацій, файлів баз даних) повинен відбуватися регулярно;
- Вимоги до конфігурування безпеки Wi-Fi мереж:
  - Зміна паролів за замовчуванням;
  - Вимкнення WPS;
  - Вимкнення SSID Broadcast;
  - Своєчасне оновлення прошивки;
  - Обмеження можливості під'єднання пристроїв до локальної мережі.

3.13. Використання робочих пристроїв

Суб'єкт повинен встановити вимоги щодо безпеки пристроїв, змінних носіїв під час їх використання.

Робочі пристрої користувачів Суб'єкта мають контролюватися централізованою системою управління.

Обов'язкове блокування екрану на пристроях після встановленого часу бездіяльності повинне бути налаштоване на всіх робочих пристроях.

Захист робочих пристроїв шляхом шифрування жорстких дисків та паролів для розблокування повинен бути реалізованим за необхідності.

Персонал несе відповідальність за забезпечення фізичної безпеки робочих пристроїв при їх використанні за межами приміщень Суб'єкта (обмеження фізичного доступу третіх сторін, слідування вимогам блокування екрану).

Забезпечення виконання вимог щодо безпечного використання робочих пристроїв має бути автоматизовано за допомогою відповідних програмних інструментів. Політики налаштування таких інструментів повинні регулярно переглядатись на відповідність даній Політиці та іншим цільовим політикам діяльності Суб'єкта.

3.14. Встановлення безпечних оновлень

В діяльності Суб'єкта повинна встановити вимоги щодо встановлення оновлень на всіх ІА, з яких надається доступ до інформації/послуг/ресурсів ТГ.

Режим автоматичного оновлення виправлень або можливість зробити це вручну має бути забезпечена адміністратором систем. Антивірусне програмне забезпечення та інші компоненти безпеки повинні регулярно перевірятись та оновлюватись до останньої версії.

Перед встановленням оновлень на виробничі системи необхідно проводити тестування оновлень в окремому тестовому середовищі.

Суб'єкт повинен проводити періодичний огляд на веб-сайті постачальника, який надає інформаційні активи на наявність оновлень.

Якщо операційна система – Windows, інструмент управління виправленнями повинен бути налаштований таким чином, щоб він автоматично завантажував останні виправлення безпеки Microsoft. Перевірка та застосування виправлень повинна проводитись за необхідності.

Адміністратор систем відповідальний за затвердження всіх виправлень та відповідальний за всі технічні зміни конфігурацій та операційних систем, програмного забезпечення, антивірусних оновлень, своєчасного встановлення виправлень та драйверів для мережевих пристроїв, робочих станцій.

3.15. Обмеження встановлення програмного забезпечення

Правила до встановлення програмного забезпечення користувачами повинні бути визначені та впроваджені Суб'єктом.

Суб'єкт повинен створити та застосовувати правила щодо дозволеного для встановлення програмного забезпечення та контролю, базуючись на принципі мінімальних привілеїв. Відповідальна особа за ІБ та адміністратор систем мають створити списки дозволеного та забороненого для встановлення програмне забезпечення.

Встановлення програмного забезпечення повинно бути обмежене для всіх користувачів, проте можливі винятки, які повинні бути схвалені адміністратором систем та Відповідальною особою за ІБ.

Функція контролю закріплена за Відповідальною особою за ІБ.

3.16. Захист від шкідливого ПЗ

Лише програмне забезпечення, затверджене адміністратором систем та Відповідальною особою за ІБ, дозволено встановлювати на системи Суб'єкта.

Сканери проти шкідливого ПЗ необхідно налаштувати на автоматичне сканування відповідних компонентів відразу після випуску оновлень.

Суб'єкт має налаштувати антивірусне програмне забезпечення на: сканування під час завантаження, сканування файлових та поштових серверів принаймні один раз на день та будь-яких інших серверів – принаймні раз на тиждень, сканування файлів при відкритті, сканування вкладень вхідної та вихідної електронної пошти,

веб сканування вмісту при синхронізації із скануванням портативних пристроїв, де це можливо.

Управління та перегляд журналів антивірусного програмного забезпечення має здійснюватися адміністратором систем.

Для захисту програмного забезпечення від шкідливих програм Суб'єкта повинно здійснюватися: ручне/автоматичне та планове сканування, видалення заражених файлів, розміщення заражених файлів на карантин, які неможливо видалити, можливість автоматичного та запланованого оновлення, реєстрація випадків шкідливого програмного забезпечення та забезпечення можливості аналізу логів, централізоване управління та ведення логів.

Комп'ютери, у яких виявлено шкідливе програмне забезпечення, та комп'ютери без антивірусного програмного забезпечення заборонено під'єднувати до мережі Суб'єкта.

Адміністратор систем повинен періодично перевіряти на веб-сайті постачальника інформаційних активів на наявність відповідних оновлень. Адміністратор систем має налаштовувати режим автоматичного оновлення патчів або робити це вручну.

Відповідальність за контроль дотримання захисту від шкідливого ПЗ покладено на Відповідальну особу за ІБ.

3.17. Управління потужностями

Суб'єкт повинен відстежувати, налаштовувати використання ресурсів та складати прогнози щодо майбутніх вимог до потужності, щоб забезпечити необхідну продуктивність систем.

Відповідальними співробітниками Суб'єкта має проводитись регулярно аудит потужностей. Вимоги до нього повинні бути визначені відповідно до пріоритету інформаційної системи для діяльності Суб'єкта.

Особливу увагу слід приділити дороговартісним ресурсам , або таким, що потребують багато часу на отримання/відновлення. Адміністратор систем та Відповідальна особа за ІБ несуть відповідальність за моніторинг ключових показників ефективності систем.

3.18. Віддалений доступ

Інтернет-ресурси Суб'єктом мають використовуватися для дистанційного виконання робочих завдань, інформаційно-аналітичної роботи в інтересах Суб'єкта, обміну поштою із третіми сторонами.

Інше використання Інтернет-ресурсів слід розглядати як порушення.

Підключення до мережі Інтернет в Суб'єкта повинно здійснюватися адміністратором систем у порядку надання прав доступу. При переміщенні співробітника (звільненні, переведенні в інший підрозділ) його безпосередній Керівник повинен подати заяву на скасування прав доступу.

Віддалене підключення до інформаційних активів Суб'єкта має здійснюватися

за допомогою визначених адміністратором систем та Відповідальною особою за ІБ ресурсів.

З'єднання веб-зустрічей/віддаленого управління (наприклад, TeamViewer, AnyDesk) не повинні використовуватися в мережі Суб'єкта для надання віддаленого доступу третім особам за замовчуванням. Цей тип підключень дозволений лише для технічного обслуговування та усунення несправностей систем після належної авторизації.

3.19. Резервне копіювання

Резервне копіювання повинно здійснюватися регулярно.

Критично важлива інформація, програмне забезпечення та системи, що підлягають резервному копіюванню, повинні бути визначені.

Періодичність створення резервних копій та частота їх тестування повинні бути чітко визначені.

Тип резервного копіювання (повне, інкрементне, диференційоване) повинен бути визначений адміністратором систем для кожної системи.

Резервні копії повинні зберігатися окремо від основних копій та повинен бути забезпечений належний рівень безпеки, а доступ до резервних копій повинен бути обмежений на тому ж рівні, що і для основних копій.

Відповідальність за здійснення резервного копіювання покладається на Відповідальну особу за ІБ.

3.20. Безпека комунікацій

Суб'єкт повинен визначити дозволені методи для зв'язку (передачі корпоративної інформації) всередині Суб'єкта та з третіми особами.

Обов'язковою є перевірка вкладень з поштових скриньок та інших месенджерів перед завантаженням.

Заборонений доступ до ресурсів Суб'єкта за прямим посиланням.

Під час обміну інформацією повинні використовуватись лише захищені протоколи передачі даних.

В Суб'єкта повинен бути впроваджений та підтримуватись процес електронного спілкування, включаючи питання безпеки, відповідно до рівня конфіденційності переданої інформації. Там, де це необхідно, повинні бути впроваджені додаткові засоби захисту (цифровий підпис, шифрування тощо).

3.21. Управління вразливостями

Інформацію про технічні вразливості використовуваних інформаційних систем слід отримувати своєчасно, оцінювати їх вплив та вживати відповідних заходів для усунення пов'язаного з цим ризику.

Оцінка вразливостей повинна проводитись регулярно та бути частиною процесу управління вразливостями. Для критичних систем та зовнішньої/внутрішньої мережі, тестування на проникнення периметру повинно проводитися періодично. Відповідальність за контроль проведення оцінки

вразливостей покладено на третю особу, а усунення вразливостей покладено на адміністратора систем та/або Відповідального співробітника за інформаційну безпеку.

3.22. Управління інцидентами

Суб'єкт повинен підтримувати План реагування на інциденти кібербезпеки (Додаток 2), який повинен спиратися на постійний оперативний моніторинг і процедури реагування на інциденти.

Суб'єкт повинен регулярно проводити навчання та підвищення обізнаності персоналу в сфері управління інцидентами. Підтримувати та розвивати процес реагування на всі типи інцидентів ІБ, відповідно до **Політики реагування на інциденти кібербезпеки (Додаток 1)**.

Кожен співробітник несе відповідальність за повідомлення Відповідальної особи за ІБ, коли він або вона дізнаються про те, що стався або міг статися інцидент ІБ, який міг поставити під загрозу безперервність діяльності Суб'єкта.

Співробітники та треті особи можуть намагатися вирішити інциденти ІБ лише за вказівками та з прямого дозволу Відповідальної особи за ІБ.

З міркувань безпеки та технічних міркувань Суб'єкт залишає за собою право відстежувати, записувати та реєструвати все використання своїх інформаційних активів і діяльність у мережі Суб'єкта.

3.23. Безперервність діяльності

Суб'єкт повинен забезпечити наявність необхідних ресурсів для безперервної діяльності та швидкого відновлення критичних систем у разі непередбачуваних ситуацій.

Керівники підрозділів несуть відповідальність за визначення вимог щодо захисту доступності систем/сервісів/даних і несуть остаточну відповідальність за їх виконання. Вимоги мають базуватися на аналізі ризиків, критичності активів і враховувати нормативні вимоги. Керівництво несе відповідальність за забезпечення необхідного фінансування для їх реалізації. Відповідальна особа за ІБ повинна забезпечувати та підтримувати безперервність систем на випадок непередбачених обставин.

Можливості аварійного відновлення особливо вразливі до збоїв і не повинні вважатися прийнятними, якщо вони не проходять регулярні задокументовані випробування.

4. Перегляд, оновлення та розповсюдження

Політика буде опублікована у формі, яку неможливо легко змінити, і у формі, яка є актуальною, доступною та зрозумілою для цільового читача. Політика зберігається та є легкодоступною для персоналу та третіх осіб (за необхідності) для подальшого використання.

Політика буде розповсюджена в електронній та паперовій формі. Нова копія Політики буде поширена разом із новою версією будь-якого компонента Політики.

Нова копія матиме збільшений номер версії.

Відповідальність за керування та оновлення Політики покладено на Відповідальну особу за ІБ. Оновлена Політика подається до Керівництва Суб'єкта для остаточного затвердження. Політика переглядається щорічно для забезпечення її адекватності та відповідності потребам і цілям Суб'єкта або частіше, якщо це необхідно (під час внесення суттєвих змін).

Керуючий справами
виконавчого комітету Олег ВОВКУН

Додаток 1
до Політики інформаційної безпеки

Політика управління інцидентами кібербезпеки

1. Загальне

Політика управління інцидентами кібербезпеки (далі – Політика) визначає вимоги та послідовність дій щодо виявлення, аналізу та опрацювання інцидентів кібербезпеки (далі – КБ) у виконавчих органах підприємствах закладах та установах Рогатинської міської ради (далі – Суб'єкт).

Метою Політики є забезпечення:

- Організація оперативного виявлення, оцінки та реагування на інциденти КБ;
- Мінімізації наслідків інцидентів КБ;
- Запобігання інцидентам КБ в майбутньому, поліпшення впровадження та використання захисних заходів КБ;
- Відповідності рівня КБ Суб'єкта вимогам законів України та інших нормативно-правових актів України, міжнародних стандартів у сфері КБ;
- Захисту інформаційних систем Суб'єкта від порушень конфіденційності, цілісності, доступності та спостережності.

1.1. Класифікація інцидентів

За наслідками інциденти КБ повинні класифікуватись за відповідно до таблиці, яка наведена у **пункті 2.2.3** даної Політики.

1.2. Види інцидентів

В цій Політиці визначені наступні види інцидентів:

- Порушення цілісності інформації;
- Порушення конфіденційності;
- Порушення доступності;
- Порушення спостережності.

2. Реагування на інциденти КБ

Етап реагування на інциденти КБ в інформаційних системах Суб'єкта повинен включати наступні кроки:

- Підготовка;
- Виявлення та аналіз;
- Стримування;
- Усунення;
- Відновлення;
- Аналіз ефективності.

2.1. Підготовка

Для забезпечення готовності Суб'єкта до оперативного реагування на інциденти КБ повинні бути розроблені плани реагування на окремі види інцидентів КБ, що є найбільш ймовірними для певної прикладної системи з урахуванням умов та режиму

її функціонування виходячи з прогнозованих даних та експертних оцінок.
Розробка планів реагування на інциденти КБ є основою для системного підходу до процесу управління інцидентами КБ в Суб'єкта.

2.1.1. Етап «Створення плану реагування на інцидент КБ»

Відповідальна особа за ІБ повинна проводити пошук інформації про аналогічні інциденти КБ, які відбувалися в минулому та для яких розроблено типовий план реагування.

Якщо для поточного виду інциденту КБ у базі знань існує типовий план реагування, то Відповідальна особа за ІБ переходить до його реалізації.

Якщо подібних інцидентів КБ у базі знань немає, Відповідальна особа за ІБ повинна розробити комплекс заходів, який оформлюється у вигляді плану реагування на інцидент КБ та зберігається в базі знань.

2.2. Виявлення та аналіз

2.2.1. Етапи «Виявлення та інформування про інцидент. Збір та реєстрація інформації про інцидент КБ»

У разі виявлення інциденту або слабких місць КБ працівники Суб'єкта або залучені треті сторони повинні повідомити про це Відповідальну особу за ІБ.

До основних ознак інциденту відносяться наступні (невичерпний перелік):

- Суттєве зниження продуктивності прикладних систем або недоступність прикладних систем;
- Повідомлення антивірусного ПЗ;
- Несанкціонована діяльність у мережі та прикладних системах Суб'єкта;
- Стрімке збільшення мережевого трафіку;
- Численні повідомлення про помилки та збої;
- Зафіксовані спроби підбору паролів;
- Заздалегідь відома негативна подія безпеки;
- Подія безпеки, що зафіксована у неробочий час;
- Невідомі облікові записи;
- Відключені засоби забезпечення безпеки;
- Спроби застосування методів соціальної інженерії;
- Відсутність засобів захисту інформації;

Працівник Суб'єкта, який виявив можливі ознаки інциденту, повинен вказати у повідомленні наступну інформацію:

- Опис проблеми, що спостерігається;
- Час виникнення ознак інциденту;
- Інші суттєві дані щодо інциденту – у відповідь на запитання Відповідальної особи за ІБ.

2.2.2. Етап «Аналіз інциденту»

Процедура повинна розпочинатись за фактом отримання Відповідальною особою за ІБ повідомлення про виникнення інциденту КБ.

Після отримання повідомлення про інцидент Відповідальна особа за ІБ повинна провести класифікацію інциденту, аналіз зібраної інформацію та прийняти рішення щодо підтвердження його статусу.

2.2.3. Етап «Оповіщення про інцидент»

В Суб'єкта оповіщення його керівників для реагування на комп'ютерні надзвичайні події повідомляється комісія CERT-UA, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний координаційний центр кібербезпеки при РНБО України, залучені треті сторони – відповідно до договірних вимог, тощо) повинно здійснюватися Відповідальною особою за ІБ визначеними засобами після маркування.

Маркування повинно проводитися відповідно до наступних значень:

Мітка (колір)	Значення
рівень некритичний (білий)	Кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних
	систем, технологічних систем.
рівень низький (зелений)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.
рівень середній (жовтий	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою.

рівень високий (помаранчевий)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб'єкта національної системи кібербезпеки.
рівень	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох

критичний (червоний)	інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки.

рівень надзвичайний (чорний)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

2.3. Стримування

2.3.1. Етап «Збір інформації для розслідування інциденту»

Відповідальна особа за ІБ відповідно до плану реагування повинна зібрати інформацію про інцидент для проведення подальшого розслідування.

У випадку, коли при реалізації збору інформації про інцидент КБ планується переривання роботи інформаційно-комунікаційної системи (далі ІКС), Відповідальна особа за ІБ, повинна погодити таке переривання з Керівництвом Суб'єкта.

2.3.2. Етап «Зменшення впливу інциденту»

Відповідальна особа за ІБ повинна обрати методи та заходи, спрямовані на зменшення впливу інциденту на процеси діяльності Суб'єкта, окремо для кожного конкретного інциденту, залежно від його виду, та у відповідності з розробленим, планом реагування.

Будь-які методи, дії та порядок їхнього використання або виконання повинні погоджуватися Керівництвом Суб'єкта.

Відповідальна особа за ІБ повинна виконати оцінку можливого впливу запланованих дій на безперервність діяльності ураженої системи та проінформувати Керівництво Суб'єкта. За необхідності допускається ізолювання системи або роз'єднання компонентів цієї системи на період проведення повного розслідування інциденту.

2.4. Усунення інциденту та відновлення функціонування інформаційно-комунікаційної системи

З метою відновлення нормального функціонування ІКС Відповідальна особа за ІБ повинна проводити заходи з усунення причин та наслідків інциденту.

Процедура усунення інциденту та відновлення функціонування залежить від

виду інциденту та повинна визначатись для кожного інциденту окремо.

Після відновлення функціонування ІКС Відповідальна особа за ІБ має перевірити відсутність ознак повторення інциденту та повідомити про завершення робіт Керівництво ТГ.

2.5. Аналіз ефективності заходів з реагування на кіберінциденти/кібератаки

2.5.1. Етап «Розслідування інциденту»

Під час виконання робіт з розслідування інцидентів повинні використовуватись методи та засоби, що запобігають випадковому або навмисному внесенню змін в дані, що вивчаються та аналізуються.

Відповідальна особа за ІБ повинна з'ясувати причини інциденту та провести аналіз усіх виявлених у процесі розслідування небезпечних факторів, що призвели до відхилень:

- у діях працівників Суб'єкта;
- у роботі інформаційних ресурсів та систем;
- відхилень від норм експлуатації програмного забезпечення і обладнання;
- відхилень від вимог політик ІБ із визначенням ступеня впливу цих відхилень на розвиток інциденту.

Відповідальна особа за ІБ повинна визначити:

- які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, розділи, пункти нормативних актів);
- причетність до інциденту, якщо це мало місце, інших підприємств, організацій і установ із визначенням, наскільки це можливо;
- ступеня їх впливу на виникнення і перебіг інциденту.

2.5.2. Етап «Аналіз ефективності»

Після завершення розслідування Відповідальна особа за ІБ повинна підготувати звіт з описом всіх проведених процедур щодо управління інцидентами КБ та закриттям інциденту КБ та надати Керівництву Суб'єкта, а також, за необхідності, зацікавленим особам.

Відповідальна особа за ІБ повинна внести інформацію про закриття інциденту в журнал реєстрації інцидентів.

3. Система внутрішнього контролю

Всі співробітники Суб'єкта несуть відповідальність за своєчасність інформування Відповідальної особи за ІБ у разі виявлення ознак інцидентів КБ або можливості настання інциденту КБ.

4. Підтримка, оновлення та розповсюдження

Політика буде опублікована у формі, яку неможливо легко змінити, і у формі, яка є актуальною, доступною та зрозумілою для цільового читача. Політика зберігається та є легкодоступною для персоналу та третіх осіб(за необхідності) для подальшого використання.

Політика буде розповсюджена в електронному та паперовому вигляді. Нова

копія Політики буде поширена разом із новою версією будь-якого компонента Політики. Нова копія матиме збільшений номер версії..

Відповідальність за керування та оновлення Політики покладено на Відповідальну особу за ІБ. Оновлена Політика подається до Керівництва Суб'єкта для остаточного затвердження. Політика переглядається щорічно для забезпечення її адекватності та відповідності потребам і цілям ТГ або частіше, якщо це необхідно (під час внесення суттєвих змін).

Керуючий справами
виконавчого комітету Олег ВОВКУН

Додаток 2
до рішення виконавчого комітету
Рогатинської міської ради від 25
листопада 2025 року №____

План реагування на інциденти кібербезпеки

Опис інциденту кібербезпеки

№	Назва інцидент у	План дій щодо реагуванн я на інцидент	Дата/час виконання дій з реагування	Очікувана дата завершення всіх дій з реагування	Технічні, програмні та фінансові ресурси	Місце збереження інформацій них підтвердже нь та доказів	Відповідаль на за реагування особа (ПІБ,Посада)	Статус			Коментарі
								Не розпочато	У процесі	Завершен о	

Приклади реагування на інцидент кібербезпеки

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
ФІШИНГ	Завдання: Визначити та впровадити кроки з розслідування інцидентів КБ, включаючи основні питання та стратегії фішингу. 1. Сфера та масштаб атаки 2. Аналіз повідомлень 3. Аналіз посилань та вкладень 4. Категоризація типу атак 5. Визначення критичності атаки	Спланувати заходи з усунення інцидентів у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Визначити необхідний час і компромісні підходи для усунення наслідків. Завдання:	Завдання: Визначити етапи проведення комунікацій під час фішинг атаки. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення після фішинг атаки. Визначити та вказати інструменти та процедуру для кожного кроку	Приклад: Дії користувача при ймовірній фішинговій атаці Завдання: Визначити кроки для користувачів, які мають підозру на фішинг.	

		Визначити тактичні та стратегічні кроки стримування фішингових атак.			
ПРОГРАМИ-ВИМАГАЧІ	Завдання: Визначити та впровадити кроки з розслідування атак/інцидентів, які відбулись за участі програм-вимагачів, зокрема основні питання та стратегії. 1. Визначити тип програм-вимагачів 2. Визначити область застосування 3. Оцінка впливу 4. Знайти інфікованого	Спланувати заходи з усунення інцидентів, у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту. Завдання: Визначити	Завдання: Визначити етапи проведення комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку. Не рекомендовано платити викуп: це не гарантує вирішення проблеми. Все може піти не так (наприклад, помилки можуть зробити дані неможливими для відновлення навіть за допомогою ключа). Крім	Приклад: Дії користувача при підозрі про наявність програми-вимагача Завдання: Визначити кроки для користувачів, які реагують на наявність програми-вимагача.

		тактичні та стратегічні кроки стримування програм-вимагачів.		того, оплата доводить, що програми- вимагачі працюють і можуть посилити атаки проти вас чи будь-кого іншого.		
АТАКА НА ВЕБСАЙТ	1. Негайно відключити зіпсований сервер для подальшого дослідження. 2. Визначити джерело вразливості системи, яку використав зловмисник. 3. Зібрати будь-які підказки щодо того, ким є хакер або на яку організацію він працює. 4. Зібрати іншу важливу	Спланувати заходи з усунення проблем, у яких кроки зі стримування запускаються разом (або скоординовано) з задіянням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з	Завдання: Визначити кроки проведення етапу комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку.	Приклад: Дії користувача при атаці пошкодження веб-сайту Завдання: Визначити кроки для користувачів, які реагують на атаку на веб-сайт.	Завдання: Поспілкуватись з іншими співробітниками, щоб переконатися, що всі розуміють наступні кроки та роблять свій внесок, де це можливо.

	інформацію зі сторінки, яка була зіпсована.	усунення інциденту. Завдання: Визначити тактичні та стратегічні кроки стримування пошкодження веб-сайтів. 1. Створити резервну копію всіх даних, що зберігаються на веб-сервері. 2. Обов'язково тимчасово вимкнути сервер зіпсованої сторінки, поки триває розслідування. 3. Після визначення джерела атаки виконати необхідні кроки, щоб переконатися, що				

		сценарій атаки більше не повториться.				

	ПІДГОТОВКА	РОЗСЛІДУВАННЯ	АНАЛІЗ	ВИПРАВЛЕННЯ	ВІДНОВЛЕННЯ	ПІСЛЯ ІНЦИДЕНТУ
ВТРАТА ДАНИХ	Забезпечити належний доступ до будь-якої необхідної документації та інформації, включаючи доступ у неробочий час, для наступного: - Процес управління інцидентами; - Схеми архітектури мережі; - Діаграми потоку даних; Визначити та отримати послуги	Завдання: Визначити та впровадити кроки з розслідування, зокрема основні питання та стратегії компрометації, ідентифікації та доступу.	1. Переконатись, що будь-які задіяні дані. 2. Проаналізувати будь-який підозрілий мережевий трафік. 3. Переглянути журнали безпеки та доступу, сканування вразливостей і будь-які автоматизовані результати інструментів. 4. Проаналізувати будь-яку підозрілу	Етап виправлення: - Містить технічний механізм порушення даних; - Усунення технічного механізму витоку даних; - Відновлення уражених систем і служб та приведення до звичайного стану.	На додаток до загальних кроків і вказівок у плані реагування на інцидент: 1. Відновити системи на основі аналізу впливу на діяльність і критичності діяльності. 2. Здійснити повне антивірусне та розширене сканування шкідливих програм усіх систем по всій організації.	Етап заходів після інциденту має такі цілі: - Заповнити Звіт про інцидент, включаючи всі деталі інциденту та дії. - Завершити процес управління інцидентами. - Опублікувати відповідні внутрішні та зовнішні повідомлення.

	стороннього провайдера. Переглянути останні кіберінциденти та їх результати.		активність, файли чи виявлені зразки ЗПЗ. 5. Зіставити будь-які нещодавні події безпеки або ознаки компрометації з підозрілою активністю в мережі. 6. Визначити джерело компрометації даних. 7. Визначити конкретний набір даних, який було зламано, а також спосіб його зламу. 8. Визначити методологію атаки та графік кіберінцидентів.		3. Повторно встановити облікові дані всіх задіяних систем і дані облікових записів користувачів. 4. Реінтегрувати раніше скомпрометован і системи. 5. Відновити будь-які пошкоджені або знищені дані. 6. Відновити усі призупинені служби. 7. Встановити моніторинг для виявлення подальшої підозрілої діяльності. 8. Координувати впровадження будь-яких необхідних виправлень або	

					заходів з усунення вразливостей.	

Керуючий справами
виконавчого комітету Олег ВОВКУН

АРКУШ

погодження до рішення виконавчого комітету

Рогатинської міської ради

Назва рішення: «Про затвердження
Політики інформаційної безпеки
та Плану реагування на кіберінциденти»

ПІДГОТОВЛЕНИЙ: відділом забезпечення
роботи інформаційно-комунікаційних систем
виконавчого комітету міської ради

ВИКОНАВЕЦЬ:
Провідний спеціаліст відділу — Богдан СЛАБИЙ

ПОГОДЖЕНО:

Перший заступник
міського голови — Микола ШИНКАР

Начальник відділу забезпечення роботи
інформаційно-комунікаційних систем
виконавчого комітету міської ради — Роман ГАВРИЛЮК

Начальник відділу правової роботи
виконавчого комітету міської ради — Світлана КОСТЬ

Керуючий справами — Олег ВОВКУН

Пояснювальна записка
до рішення виконавчого комітету Рогатинської міської ради
«Про затвердження Політики інформаційної безпеки
та Плану реагування на кіберінциденти»

1. *Обґрунтування необхідності прийняття рішення*

Необхідність прийняття даного рішення зумовлене зростанням кількості та складності кіберзагроз, що можуть становити небезпеку для функціонування інформаційно-комунікаційних систем органу місцевого самоврядування.

2. *Мета прийняття рішення*

Метою даного рішення є визначення чіткого алгоритму дій у разі виявлення кіберінцидентів, забезпечення швидкого реагування та мінімізація наслідків атак, встановити відповідальних осіб та структури, залучені до реагування.

3. *Правові аспекти*

Дане рішення розроблено відповідно до п. 20 ч. 4 ст. 42, ч. 8 ст. 59 Закону України «Про місцеве самоврядування в Україні» від 21.05.1997 №280/97-ВР, Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII, Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року, введеного в дію Указом Президента України від 01 лютого 2022 року №37/2022, Порядку реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затвердженого постановою Кабінету Міністрів України від 04 квітня 2023 року №299.

4. *Фінансово-економічне обґрунтування*

Рішення не потребує фінансування.

5.Громадське обговорення

Рішення не потребує громадського обговорення.

6.Прогноз результатів

Прийняття даного рішення забезпечить загальний рівень кіберстійкості інформаційно-комунікаційних систем ради та її виконавчих органів, комунальних підприємств, установ і закладів.

7.Оприлюднення

Рішення виконавчого комітету Рогатинської міської ради потребує оприлюднення.

Провідний спеціаліст
відділу забезпечення роботи
інформаційно-комунікаційних систем — Богдан СЛАБИЙ