УДК 351.746:007
DOI: 10.35432/tisb292023289764

ВАЖЛИВІСТЬ КІБЕРБЕЗПЕКИ ДЛЯ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ

Ткачук Дарія Миколаївна
здобувач
Інститут публічної служби та управління
Національний університет «Одеська політехніка»
https://orcid.org/0009-0000-6761-2464

У нашому сучасному цифровому світі, де зростає кількість кібератак, важливість кібербезпеки для органів місцевого самоврядування (ОМС) є надзвичайно високою. Це пов'язано з тим, що ОМС забезпечують найважливіші соціальні та інфраструктурні послуги для місцевих жителів, такі як медичні послуги, енергопостачання, транспорт, водопостачання та інші, тому вони повинні бути захищені від кіберзагроз.

Для забезпечення високого рівня кібербезпеки, ОМС мають вживати широкого спектру заходів. Перш за все, вони повинні встановлювати сучасні системи кіберзахисту для захисту своїх мереж та інформації. Крім того, вони мають розробляти та впроваджувати стратегії кібербезпеки, які відповідають їхнім конкретним потребам та загрозам.

Органи місцевого самоврядування також повинні забезпечити навчання своїх співробітників кібербезпеці та кібергігієні. Це може включати проведення тренінгів та навчання з кібербезпеки, створення внутрішніх політик та процедур щодо захисту інформації та регулярне оновлення програмного забезпечення та апаратного забезпечення, які використовуються для обробки даних та зберігання інформації.

Окрім того, ОМС повинні дотримуватися нормативно-правових актів з кібербезпеки, які встановлені урядом та іншими компетентними органами. Наприклад, Україна має закон «Про основні принципи забезпечення кібербезпеки України», прийнятий у 2017 році, який встановлює основні принципи кібербезпеки, визначає структуру управління кібербезпекою та встановлює вимоги до захисту інформації.

Узагалі, відповідальність за забезпечення кібербезпеки ОМС є надзвичайно важливою, оскільки вони мають доступ до значної кількості конфіденційної інформації про місцевих жителів та інфраструктуру, що може стати об'єктом кібератак. У разі порушення кібербезпеки, ОМС можуть стати жертвами різних типів кіберзлочинів, включаючи втрату даних, викрадення конфіденційної інформації та інших негативних наслідків. [2]

Отже, високий рівень кібербезпеки є критичним для забезпечення надійної та безпечної роботи органів місцевого самоврядування.

Застосування відповідних технологій та політик кібербезпеки є ефективним способом зменшення ризику кіберзагроз та забезпечення захисту від потенційних кібератак на ОМС. Для забезпечення кібербезпеки, ОМС можуть застосовувати такі технології та практики, як: [2]

1. Використання захищеного програмного забезпечення та апаратного забезпечення, які мають вбудовані механізми захисту від кіберзагроз. Це може включати використання антивірусного програмного забезпечення, брандмауерів, інтрузійних виявників та інших захисних інструментів.

2. Застосування сучасних методів шифрування та захисту даних, які забезпечують конфіденційність та цілісність інформації.

3. Регулярне оновлення програмного забезпечення та апаратного забезпечення, які використовуються для обробки даних та зберігання інформації.

4. Створення внутрішніх політик та процедур щодо захисту інформації, які включають плани дій у разі кібератак та інші заходи для забезпечення безпеки.

5. Проведення тренінгів та навчання з кібербезпеки для персоналу ОМС, що дозволить забезпечити високий рівень свідомості про кібербезпеку та допоможе уникнути потенційних загроз.

6. Використання моніторингових інструментів, які дозволяють виявляти потенційні загрози та забезпечують оперативну реакцію на кібератаки.

Застосування цих технологій та практик може допомогти ОМС уникнути потенційних кібернетичних загроз та зменшити ризик кібератак на їхні системи та мережі. Важливо пам'ятати, що злочинці постійно шукають нові способи атаки на системи та мережі, тому важливо проводити оновлення технологій та практик кібербезпеки, щоб залишатися в курсі нових загроз та протидіяти їм.

Також важливо звернути увагу на законодавчий аспект кібербезпеки в ОМС. Нормативно-правові акти, які регулюють питання кібербезпеки включають закони, постанови та розпорядження, які встановлюють правила та процедури для захисту інформації в ОМС. Наприклад, Український Закон «Про кібербезпеку» від 5 липня 2017 року встановлює правові засади забезпечення кібербезпеки в Україні та визначає права та обов'язки суб'єктів кібербезпеки.

Нормативно-правові акти також встановлюють вимоги щодо захисту інформації та персональних даних, що зберігаються в ОМС. Наприклад, «Положення про захист інформації в Органах місцевого самоврядування» зобов'язує ОМС забезпечувати захист конфіденційної інформації та персональних даних, які збираються та обробляються в ОМС.

У разі порушення правил та вимог, встановлених нормативно-правовими актами, можуть бути запроваджені адміністративні та кримінальні відповідальності. Тому важливо для ОМС враховувати вимоги нормативно-правових актів щодо кібербезпеки та вживати всіх необхідних заходів для їх виконання.

Отже, дотримання вимог нормативно-правових актів та застосування сучасних технологій та практик кібербезпеки може значно зменшити ризики кіберзагроз та забезпечити захист від потенційних кібератак на ОМС.

При використанні технологій та практик кібербезпеки, важливо мати на увазі, що це не просто про технічні рішення, але про впровадження комплексу заходів, що забезпечують захист від різних типів кіберзагроз. Для цього необхідно створювати комплексні програми кібербезпеки, які містять в собі не тільки технічні рішення, а й процедури та правила, що регулюють доступ до інформації, розподіл відповідальності між працівниками ОМС, плани дій в разі виявлення загроз, та інші компоненти. [5]

До технічних засобів кібербезпеки можуть відноситися антивірусні програми, файрволи, інтегровані системи захисту, системи моніторингу та виявлення інцидентів, шифрування даних тощо. На додаток до технічних засобів, важливо розробляти та впроваджувати процедури та правила, що забезпечують безпеку інформації в ОМС. Наприклад, необхідно встановлювати строгі правила щодо створення та зберігання паролів, обмежувати доступ до важливої інформації лише необхідним працівникам та використовувати засоби двофакторної аутентифікації.

Також дуже важливо, щоб працівники ОМС мали достатній рівень знань з питань кібербезпеки. На жаль, багато працівників ОМС не мають достатньої освіти та навичок у цій галузі, що може призвести до вразливості ОМС перед кібератаками. Тому, регулярні тренінги та навчання для працівників ОМС є критичними для забезпечення кібербезпеки.

Тренінги та навчання мають на меті підвищення рівня свідомості та навичок працівників ОМС з питань кібербезпеки. Вони можуть бути проведені як внутрішньо у ОМС,

так і за їх межами, залежно від потреб та можливостей. Зокрема, працівників ОМС можна навчати: [5]

- розпізнавати кіберзагрози та кібератаки;
- застосовувати відповідні технології та політики кібербезпеки;
- створювати складні паролі та застосовувати двофакторну аутентифікацію;
- виявляти та відновлювати дані після кібератак;
- зберігати конфіденційну інформацію та захищати її від несанкціонованого доступу.

Регулярні тренінги та навчання також можуть допомогти ОМС виявляти та усувати слабкі місця в системах кібербезпеки, що може знизити загрозу кібератак.

Одним з прикладів успішного навчання та тренінгів з кібербезпеки для ОМС є програма «Інформаційна безпека для місцевих органів влади» від Європейського союзу. Програма була розроблена з метою підвищення рівня кібербезпеки для місцевих органів самоврядування та включає в себе такі елементи: [3]

1. Аналіз загроз та оцінка ризиків – цей етап дозволяє визначити, які типи кіберзагроз можуть стати найбільшими ризиками для ОМС та які заходи потрібно вжити для їх запобігання.

2. Розробка та впровадження політик кібербезпеки – цей етап передбачає розробку політик та процедур, що стосуються захисту від кіберзагроз та їх впровадження в робочі процеси ОМС.

3. Кібергігієна - цей етап включає навчання та тренінги працівників ОМС з питань кібербезпеки, а також створення культури безпеки та практик кібергігієни серед працівників ОМС.

4. Захист мереж та інфраструктури – цей етап передбачає встановлення захисних систем на мережах та серверах ОМС, що дозволить запобігти кібератакам та забезпечити безпеку важливих даних.

5. Моніторинг та виявлення кіберзагроз – цей етап дозволяє вчасно виявляти потенційні кіберзагрози та реагувати на них.

6. Реагування на кібератаки – цей етап передбачає планування та розробку процедур реагування на кібератаки та відновлення роботи систем після їх проведення.

7. Аудит безпеки – цей етап передбачає проведення регулярних аудитів безпеки, що дозволяють оцінювати ефективність вжитих заходів та виявляти слабкі місця в системі кібербезпеки ОМС.

Усі ці етапи взаємопов’язані та доповнюють один одного, що дозволяє забезпечити високий рівень кібербезпеки для ОМС. Проте, важливо зазначити, що це процес, який потребує постійного вдосконалення та адаптації до нових загроз та викликів. Крім того, необхідно забезпечити своєчасне оновлення обладнання та програмного забезпечення, щоб забезпечити захист від нових вразливостей та використання новітніх технологій у кібербезпеці.

Узагалі, питання кібербезпеки стає все важливішим для ОМС, оскільки вони мають велику кількість конфіденційної інформації, такої як персональні дані громадян, фінансові та інші документи. Тому, в разі порушення кібербезпеки можуть виникнути значні наслідки, які можуть підірвати довіру громадян до діяльності ОМС та порушити їх роботу.

Отже, високий рівень кібербезпеки є критично важливим для ОМС, і необхідно підтримувати його за допомогою відповідної політики, технологій та навчання працівників. Це дозволить ОМС ефективно захищати свою інформацію та забезпечувати високу якість надання послуг для громадян.

Список літератури

1 Кобзева, І.В. Кібербезпека як невід’ємний елемент інформаційної безпеки. Вісник Національного університету «Львівська політехніка». Серія: Комп’ютерні науки та інформаційні технології. 2019. № 925. С. 191-198.

2 Кучеренко, О.В. Особливості організації кібербезпеки в ОМС. Науковий вісник Херсонського державного університету. Серія: Економічні науки. 2018. Вип. 28(3). С. 14-17.

3 Попова, О.Ю. Основні принципи забезпечення кібербезпеки в ОМС. Міжнародний науковий журнал «Інтернаука». 2020. № 2. С. 48-52.

4 Приймак, Т.І. Кібербезпека в ОМС: методологічний підхід. Бізнес Інформ. 2020. № 2. С. 71-76.

5 Романова, О.І. Заходи забезпечення кібербезпеки в ОМС на прикладі Одеської області. Вісник Одеського національного університету імені І.І. Мечникова. 2021. Т. 26, № 2. С. 51-56.

6 Харченко, А.І. Кібербезпека як складова інформаційної безпеки. Економічні науки. 2017. Т. 1, № 4. С. 93-98.

7 Шевченко, І.В. Кібербезпека в ОМС: виклики та перспективи. Науковий вісник Міжнародного гуманітарного університету. Серія: Юридичні науки. 2018. Вип. 28. С. 16-20.