Шестаковська Т.Л.
доктор наук з державного управління, доцент,
ректор Чернігівського інституту інформації, бізнесу і права ЗВО «МНТУ»,
м. Чернігів

ЗАХИСТ ІНФОРМАЦІЇ В ГАЛУЗІ ДЕРЖАВНОГО УПРАВЛІННЯ: ПРОБЛЕМИ ТА ПІДХОДИ В ОСВІТНІЙ СФЕРІ

В епоху постійної цифровізації та глобальних змін, забезпечення інформаційної безпеки стає ключовим елементом у сфері державного управління. Розширення використання інформаційних технологій, збільшення обсягів даних, що обробляються державними органами, а також зростання складності та різноманітності інформаційних ризиків породжують нові виклики у сфері забезпечення інформаційної безпеки в секторі державного управління.

Серед основних викликів у сфері інформаційної безпеки в публічному управлінні можна виділити такі:

1. Зростання складності і різноманітності інформаційних загроз. Кібератаки стають все більш витонченими і ефективними, а також поширюються на все нові сфери діяльності. Органам влади необхідно постійно оновлювати свої знання та навички в галузі інформаційної безпеки, щоб ефективно протистояти цим загрозам.

2. Недостатній рівень обізнаності про інформаційну безпеку серед публічних службовців. Багато публічних службовців не мають достатніх знань і навичок у галузі інформаційної безпеки, щоб ефективно захищати інформацію, з якою вони працюють. Це може призвести до випадкових помилок, які можуть бути використані для здійснення кібератак.

3. Нестача ресурсів для забезпечення інформаційної безпеки. Органи влади часто не мають достатніх ресурсів, щоб забезпечити ефективне управління інформаційною безпекою. Це може призвести до того, що органи влади не зможуть повністю захистити себе від інформаційних загроз.

4. Залежність сучасного публічного управління від технологій невпинно зростає, пропонуючи величезні можливості для ефективності та інновацій.

Проте, ця залежність також вносить ряд значних викликів та ризиків: цифрова вразливість (збільшення використання цифрових технологій робить системи управління більш вразливими до кібератак. Це може включати злам даних, розповсюдження вірусів, атаки типу "відмова в обслуговуванні" (DDoS) та інші кіберзагрози); застарілі системи (часто урядові установи використовують застаріле обладнання та програмне забезпечення через обмежені бюджети або бюрократичні затримки у процесі оновлення технологій); збільшення залежності від сторонніх постачальників (публічний сектор залежить від приватних компаній, які надають технологічні послуги та рішення, що може вести до проблем з конфіденційністю та безпекою даних); складність управління даними (великі обсяги зібраних даних потребують ефективного управління, забезпечення конфіденційності, цілісності та доступності); відставання навичок співробітників (співробітники публічного сектору часто не мають необхідних навичок для роботи з сучасними технологічними системами, що вимагає інвестицій в навчання та розвиток) [1].

Одним із підходів до підвищення обізнаності про інформаційну безпеку є проведення навчальних семінарів і тренінгів для публічних службовців. Ці семінари і тренінги повинні бути спрямовані на висвітлення основних аспектів інформаційної безпеки, таких як: поняття інформаційної безпеки, основні інформаційні загрози, заходи захисту інформації.

Крім того, необхідно розробити навчальні програми з інформаційної безпеки для публічних службовців. Ці програми повинні бути спрямовані на формування у публічних службовців необхідних знань і навичок у галузі інформаційної безпеки, таких як: ідентифікація і оцінка ризиків інформаційної безпеки, розробка заходів захисту інформації, відповідь на інформаційні загрози.

Також необхідно забезпечити доступ публічних службовців до ресурсів, необхідних для ефективного управління інформаційною безпекою. Ці ресурси можуть включати: керівні документи з інформаційної безпеки, інструменти і технології захисту інформації, сервіси підтримки в сфері інформаційної безпеки.

Забезпечення ефективної освіти в сфері інформаційної безпеки для публічних службовців є важливим кроком на шляху до підвищення рівня інформаційної безпеки в державному секторі.

Формування культури безпеки є важливим аспектом захисту інформаційних систем у сфері публічного управління. Воно включає в себе ряд заходів, спрямованих на підвищення обізнаності, зміцнення відповідального ставлення до інформації та розвиток навичок безпечної поведінки серед співробітників та громадян. Ось основні кроки для ефективного формування культури безпеки:

1. Освітні та тренінгові програми. Регулярні тренінги: проведення регулярних тренінгів та семінарів з інформаційної безпеки для співробітників всіх рівнів. Симуляції: організація практичних вправ, наприклад, симуляцій фішингових атак, для розвитку навичок виявлення та реагування на кіберзагрози.

2. Політики та процедури. Розробка політик безпеки: встановлення чітких правил та стандартів поведінки у сфері обігу інформації. Аудит та моніторинг: регулярний аудит та моніторинг дотримання політик безпеки для забезпечення їх ефективності.

3. Комунікаційні кампанії. Інформаційні бюлетені та електронні листи: регулярне розсилання інформаційних матеріалів з актуальними порадами та новинами у сфері інформаційної безпеки. Інтерактивні кампанії: використання соціальних медіа та інших платформ для підвищення обізнаності про загрози та методи захисту.

4. Залучення керівництва. Приклад згори: активна участь керівництва в освітніх заходах та підтримка ініціатив з безпеки. Політика відкритих дверей: створення атмосфери, у якій співробітники можуть вільно ділитися своїми занепокоєннями та ідеями щодо поліпшення безпеки.

5. Підтримка неперервного навчання. Оновлення курсів та матеріалів: регулярне оновлення навчальних матеріалів для відображення найновіших загроз та технологій. Мотивація до самоосвіти: створення умов для самостійного вивчення та професійного розвитку у сфері безпеки [2].

Отже, формування культури безпеки є багатогранним процесом, який вимагає залучення, освіти та постійної уваги всіх учасників процесу управління. Це не лише

про технології та процедури, але й про створення середовища, в якому безпека інформації є фундаментальною цінністю. Зростаюча загроза кібератак, потреба у захисті великих обсягів даних, та виклики, пов'язані з управлінням та оновленням IT-інфраструктури, є ключовими викликами для публічного сектору. Недостатні навички та обізнаність співробітників публічного сектору з питань кібербезпеки та технологій можуть підсилити ризики. Обмежені бюджети та потреба в оновленні застарілої IT-інфраструктури створюють фінансові та оперативні труднощі.

Список використаних джерел

1. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя. № 1. 2020. С. 102-109.

2. Organization for Security and Co-operation in Europe – OSCE. URL: https://www.osce.org/whatistheosce.