Наталія ГАЛУНЕЦЬ
старший викладач кафедри
публічного управління та адміністрування і
міжнародної економіки
Миколаївський національний аграрний університет
м. Миколаїв

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕРИТОРІАЛЬНИХ ГРОМАД В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Сучасні інформаційні технології розширюють можливості доступу до інформації, розвитку особистих компетенцій, нетворкінгу та комунікації, що особливо важливо для успішного функціонування реформи децентралізації. Водночас, у взаємопов'язаному світі миттєвої інформації, конфіденційність і інформаційна безпека є елементами перехресного вогню, який не зупиняє потік інформації.

В Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», вказано, що інформаційна безпека - це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому завдається шкода через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [1, 2].

Інформаційна безпека територіальних громад характеризується мірою захищеності громади та стійкості основних сфер життєдіяльності громади (економіки, науки, техносфери, сфери управління, військової справи і т. ін.) відносно небезпечних інформаційних впливів, причому як з упровадження, так і добування інформації.

Виходячи із сутності інформаційної безпеки основними заходами її забезпечення є:

- максимальний захист інформаційних активів підконтрольної установи;

- відповідність нормативним вимогам;

- зведення до мінімуму потенційну юридичну відповідальність і вплив на репутацію економічно ефективним способом.

В умовах воєнного стану в Україні все частіше надходять повідомлення про кібератаки від державних організацій, органів місцевого самоврядування, закладів освіти та охорони здоров'я, банків, юридичних фірм, некомерційних організацій та багатьох інших організацій.. В результаті, традиційні військові атаки та кібератаки стали частиною повсякденної діяльність держав та інших установ, для яких інформація або дезінформація («фейкові новини» або «альтернативні факти') стали зброєю. Тож, інформаційна безпека напряму пов'язана з кібератаками.

Відсутність єдиного підходу в світі до боротьби з кіберзлочинністю ускладнює здатність державних та місцевих органів визначати ризик і загрозу навколишнього середовища та вжити необхідних заходів, щоб протистояти і стримувати атаки. Це також ускладнює окреслення меж між відповідальністю державних органів чи органів місцевого самоврядування і відповідальність приватного сектора [3].

Для територіальних громад настав час створити або вдосконалити свою інформаційну політику та інформаційне середовище, що є основою інформаційної безпеки. Незалежно від того, скільки пристроїв, програм і серверів дійсно використовує громада, немає виправдання важкій і складній інфраструктурі, яка уповільнює її процеси.

Забезпечення інформаційної безпеки територіальних громад, на нашу думку, передбачає формування ієрархічності політики кожного відділу діяльності громади, а саме:

- політика інформаційної безпеки відділу бухгалтерії;

- політика інформаційної безпеки відділу управління;

- політику інформаційної безпеки відділу надання адміністративних послуг; та інші.

Визначення політики інформаційної безпеки в такий ієрархічний спосіб має багато переваг. Роблячи це, громада враховує потреби кожного відділу та гарантуєте, що їхні робочі процеси та інформація не будуть скомпрометовані в ім'я безпеки. Розроблена та затверджена письмова політика служитиме формальним посібником для всіх заходів кібербезпеки, які використовуються в територіальній громаді. Це дозволяє вашим фахівцям із безпеки та співробітникам бути на одній сторінці та дає вам можливість застосовувати правила, які захищають ваші дані.

Наступним кроком забезпечення інформаційною безпекою територіальних громад є контроль застосування Інтернет речей (IoT), який набирає популярність з року в рік. Найскладніше в пристроях IoT – це обмежити їхній доступ до конфіденційної інформації. Щоб належним чином керувати цими пристроями, подумайте про впровадження найкращих практик безпеки мережі IoT. Камери відеоспостереження, дверні дзвінки, розумні дверні замки, системи опалення, офісне обладнання - усі ці маленькі частини мережі діяльності громади є потенційними векторами атак. Наприклад, зламаний принтер може дозволити зловмисникам переглядати всі документи, які друкуються чи скануються. Тому потрібно чітко прописати правила інформаційної безпеки для забезпечення безпеки даних через використання Інтернету речей (IoT), щоб ніхто не міг увійти до пристроїв без дозволу.

Для забезпечення інформаційної безпеки територіальних громад важливо також спростити їх технологічну інфраструктуру. Забагато інструментів які використовуються в інформаційній безпеці може ускладнити виявлення загроз. Якщо інфраструктура інформаційної безпеки територіальної громади спрямована на зниження ризику витоку даних, тоді вона не повинна містити занадто багато частин і бути розділеною між різними рішеннями [4].

Наступним способом забезпечення інформаційної безпеки територіальних громад є створення захищеного доступу за допомогою ефективного керування ідентифікацією. Використовуйте біометричний захист. Як відомо біометрія забезпечує швидку автентифікацію, безпечне керування доступом і точний

моніторинг співробітників. Розпізнавання голосу, сканування відбитків пальців, біометрія долоні та поведінкова біометрія, розпізнавання обличчя та аналіз ходи є ідеальними варіантами для визначення того, чи є користувач тим, за кого себе видає. Перевірка особи користувачів перед наданням доступу до цінних активів є життєво важливою для територіальної громади.

Таким чином, використовуючи наведенні засоби територіальні громади забезпечать захист своїх даних та репутацію в інформаційному середовищі. Поряд з цим, широкий функціонал запропонованих засобів включає широкі можливості моніторингу, засобів реагування та рішення для контролю доступу, що допоможуть територіальним громадам дотримуватися більшості законів і норм у сфері інформаційної безпеки в усьому світі, включно зі стандартами банківської кібербезпеки. Така кількість функціональних можливостей в одному легкому рішенні дозволить Львівській міській територіальній громаді усунути прогалини в інформаційній безпеці та застосувати багато найкращих практик, запропонованих нами.

Список використаних джерел

1. «Про захист інформації в інформаційно-телекомунікаційних системах» : Закон України : станом на 5 лип. 1994 р. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

2. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права* : зб. наук. пр. Вип. 86 / редкол.: Г. І. Чанишева (голов. ред.) та ін. – Одеса : Гельветика, 2020. – С. 190-196.

3. Carl S. Young Information Security Science Measuring the Vulnerability to Data Compromises. *Cambridge : Syngress* 2016, Pages 339-357

4. Шемчук В. В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2019. № 4. С. 31–37. (Серія «Юридичні науки»). doi: https://doi.org/10.32838/1606-3716/2019.4/06.