населення в умовах надзвичайних ситуацій. Його зміст охоплює формування нормативно-правової бази, визначення інституційної структури та розподілу повноважень, регламентацію процесів планування і реалізації заходів реагування, а також забезпечення ресурсної та інфраструктурної готовності системи цивільного захисту [1].

Менеджмент безпеки та правове забезпечення захисту населення у надзвичайних ситуаціях утворюють цілісну систему управлінських і нормативно-правових заходів, спрямованих на зниження ризиків, попередження криз і забезпечення стійкості суспільства до загроз. Її ефективність визначається здатністю державних інституцій до оперативного реагування, координації та адаптації до змінного безпекового середовища.

Управлінський компонент передбачає реалізацію політики ризик-менеджменту, що включає виявлення загроз, оцінку їх наслідків і розроблення превентивних та реагувальних заходів на основі прогнозування. Водночас правове забезпечення формує регулятивні механізми, визначає повноваження суб'єктів, порядок взаємодії та гарантує дотримання прав людини. Результативність системи залежить від інституційної спроможності, ресурсного та інформаційного забезпечення, а також використання сучасних технологій моніторингу і оповіщення. Важливим чинником є формування культури безпеки населення та його готовності до дій у надзвичайних умовах.

У сучасних умовах система публічного управління цивільним захистом потребує переорієнтації на інноваційні управлінські моделі, що враховують динаміку технологічного розвитку, актуальні суспільні виклики та змінність безпекового середовища. Залучення потенціалу громад і поєднання їх ресурсів із державними можливостями сприяє формуванню адаптивної та стійкої системи безпеки, здатної ефективно протидіяти різним типам загроз і забезпечувати належний рівень захисту населення. Водночас міжмуніципальна взаємодія у сфері цивільного захисту виступає дієвим механізмом підвищення безпеки на локальному рівні. Вона забезпечує узгодженість дій під час реагування на надзвичайні ситуації, сприяє консолідації ресурсів територіальних громад, посиленню їхньої соціальної інтегрованості та створює передумови для довгострокового розвитку, одночасно зміцнюючи загальнонаціональну систему безпеки [2].

Список використаних джерел.

1. Феськов Я., Ковальчук О. Адміністративно-правове забезпечення менеджменту цивільного захисту. URL : https://surl.li/udlemb

Гавура А. Публічне управління у сфері цивільного захисту: нові підходи до інтеграції громадських ресурсів. URL : https://conference.wunu.edu.ua/index.php/apmpuvusv/article/download/791/736

РИЗИКИ ТА ЗАХОДИ КІБЕРБЕЗПЕКИ ДЛЯ НАСЕЛЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Шандуренко Б.Є.
Миколаївський Національний Аграрний Університет
shandurenko333123@gmail.com

Актуальність кібербезпеки в сучасних умовах безперечна, оскільки ворог систематично здійснює спроби отримати конфіденційну інформацію та намагається завдати шкоди як державним структурам, так і цивільному населенню. Під загрозою перебувають не лише офіційні установи та інформаційні ресурси, а й особисті дані

громадян. Цілі таких дій - викрадення інформації, порушення функціонування систем, поширення дезінформації з метою дестабілізації суспільства.

Серед загроз варто виділити фішинг, який розповсюджує підроблені повідомлення та посилання. Вони спонукають користувачів розкривати конфіденційні дані, зокрема паролі та персональну інформацію. Небезпечним явищем є дезінформація, яка за рахунок розповсюдження цілеспрямованих неправдивих відомостей може створити панічні настрої чи соціальну тривогу суспільства. Ще одна загроза сучасності - маніпуляції. Вони пов'язані з людською цікавістю, коли громадянам можуть пропонувати сумнівні матеріали чи завдання, що передбачають передачу чутливої інформації в обмін на винагороду.

Потенційну небезпеку становлять невідомі електронні носії інформації, зокрема флеш-накопичувачі, файли чи зображення, отримані від невідомих чи скомпрометованих джерел. Вони можуть містити шкідливе програмне забезпечення. В таких умовах важливо дотримуватися базових правил інформаційної безпеки, уникати взаємодії з підозрілими цифровими об'єктами та не відкривати невідомі посилання чи файли.

Надійний захист кібербезпеки, це впровадження ефективних механізмів захисту облікових записів та відповідальна поведінка користувачів у цифровому середовищі.

Надійним засобом захисту є двофакторна автентифікація. Вона передбачає використання не лише пароля, а й додаткового способу підтвердження особи. Такий підхід суттєво знижує ризик несанкціонованого доступу до облікового запису.

Важливим є створення складних та унікальних паролів для кожного окремого сервісу. Прості комбінації підвищують ймовірність компрометації, складні паролі, що містять різні типи символів, є значно стійкішими до підбору. Доцільно застосовувати різні паролі для різних ресурсів. Це унеможливлює доступ до інших облікових записів у разі витоку одного з них.

Обережність при взаємодії з цифровим контентом важлива. Не рекомендується переходити за посиланнями, які були отримані віз невідомих чи підозрілих джерел, навіть якщо вони надіслані знайомими, чия поведінка викликає сумніви. Міркування безпеки наголошують - не поширюйте інформацію, яка може містити чутливі данні, а також не обговорюйте такі питання через незахищені канали зв'язку.

Ризики кіберзагроз можна мінімізувати за допомогою дотримання комплексного підходу до цифрової безпеки. Важливо оновлювати програмне забезпечення пристроїв. Виробники систематично випускають оновлення програмного забезпечення, які містять виправлення вразливостей і адаптацію до нових типів атак. Треба використовувати VPN-сервіси, які сприяють підвищенню рівня конфіденційності шляхом приховування реального IP-адреса та ускладнення відстеження місцезнаходження користувача. Не менш важливим є налаштування параметрів приватності в месенджерах і соціальних мережах. Це обмежу доступ сторонніх осіб до персональної інформації та знижує ймовірність їх зловживання.

Отже, жоден цифровий інструмент не гарантує абсолютної безпеки. Для досягнення максимально можливого рівня захисту варто з обережністю ставитися до використання онлайн-комунікаційних платформ або, у разі підвищених вимог до конфіденційності, мінімізувати їх застосування.