значення похибки на порядок менше для дальньої зони сейсмолокації чим для діючого методу, в якому не враховується сферичність розповсюдження сейсмохвилі, а також на чверть базової відстані менше похибка визначення ординати об'єкта, за умови розрахунку пеленга згідно методу [2]. Крім цього, при ВМП локатором з виключенням параметра швидкості розповсюдження сейсмохвилі з розрахунків важливим етапом є вибір топології тріади сейсмодатчиків, врахування координати точки спостереження і сферичності фронту розповсюдження сейсмохвилі, що дозволяє компенсувати відповідну систематичну похибку визначення абсциси місцеположення об'єкта і зменшити до рівня половини базової відстані похибку визначення ординати місцеположення об'єкта.

У середньому похибка визначення ординати зменшена на 23 % і в 8 раз, в залежності від діючого методу, з яким порівнюється розроблений.

Список використаних джерел:

1. Morozov Y. V., Rajfeld M. A., Spector A. A., Analysis of seismic signals preliminary processing influence on classification results // 12 International forum on strategic technology (IFOST 2017) : proc., Korea, Ulsan, 31 May – 2 June 2017. Ulsan, 2017. Vol. 1. P. 138-142.

2. Прокина Н. В. Пеленгация наземных объектов с использованием сейсмических датчиков / Н.В. Прокина, В.А. Дудкин. // Датчики и системы / под. ред. Кнеллер В. Ю. – М. : ИПУ РАН, 2010. – № 1. – С. 24–29.

3. Лантвойт О.Б., І.М. Лисий, І.М. Плосконос Аналіз методів і розробка нового технічного рішення визначення місцеположення об'єкта пасивними засобами локації / О.Б. Лантвойт, М.І. // Системи озброєння і військова техніка. – 2010. – № 1(21). – С. 170-174.

4. Сайбель А. Г. Разностно-дальномерный метод радиопеленгования / Сайбель А. Г. // Радиотехника / под ред. Ю. В. Гуляева. – М. : «Радиотехника», 2003. – № 4. – С. 39–41.

д.т.н., проф. Лєнков С.В. (ВІКНУ)
к.т.н., с.н.с. Мірошніченко О.В. (ВІКНУ)
к.т.н., доц. Чешун В.М. (ХмНУ)
к.т.н., доц. Чорненький В.І. (ХмНУ)
д.т.н., доц. Яцків В.В. (ТНЕУ)

СТАНДАРТИ І ПОЛІТИКИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Цінність інформаційних ресурсів і необхідність забезпечення їх функціональної безпеки усвідомлена усіма доволі давно, але поява нових ризиків в умовах гібридної війни значно загострює проблему захисту інформаційних цінностей і забезпечення безперервності бізнес-процесів, що зумовлює потребу у застосуванні комплексного підходу до вирішення задач інформаційної безпеки сучасного підприємства.

На захист інтересів бізнесових структур на цей час розроблено велику кількість державних і міжнародних стандартів з питань інформаційної безпеки. Особливе місце серед подібних стандартів займає група міжнародних

стандартів інформаційної безпеки серії 27000х, які можуть бути застосовані організаціями усіх рівнів у будь-яких сферах діяльності [1]. Стандарти серії 27000х забезпечують багатоаспектний підхід до питань інформаційної безпеки, починаючи із загального огляду задач та введення в термінологію і завершуючи пропозиціями кращих практик впровадження, розвитку та вдосконалення системи управління інформаційною безпекою Про актуальність зазначених стандартів в сучасних умовах для бізнесу України свідчить прийняття частини з них в якості державних (ДСТУ ISO/IEC 27001-2015, ДСТУ ISO/IEC 27002:2015 тощо).

Політика інформаційної безпеки підприємства базується на багатоаспектному і комплексному підході до вирішення завдань захисту інформаційних ресурсів і повинна враховувати питання політик безпеки використання електронних сервісів та програмного-апаратного забезпечення, роботи персоналу в межах виконання посадових обов'язків, діяльності структурних підрозділів та підприємства в цілому тощо. Таким чином, ефективна політика безпеки розробляється з орієнтацією на структурну організацію підприємства, сферу і особливості його діяльності, кадровий склад, використовувані засоби та інформаційні технології.

При формуванні політики безпеки виникає питання економічної доцільності організації бажаного комплексу заходів інформаційної безпеки, оскільки витрати на систему безпеки можуть перевищити цінність об'єктів захисту. Як наслідок, необхідно враховувати, що окремі вразливості можуть зберегтися й після застосування обраних механізмів і сервісів безпеки, а тому і завдання синтезу політики зводиться до формування актуального рішення, яке безпеки визначає погоджену сукупність механізмів і сервісів безпеки, адекватну цінностям, що захищаються, і оточенню, у якому вони використовуються.

к.т.н. Муляр І.В. (ХмНУ)
к.т.н. Лєнков Є.С.
к.т.н. Лоза В.М. (ВІКНУ)
Якубець А.В. (ХмНУ)

ОСНОВНІ ПІДХОДИ ДО СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації. Система ТЗІ – сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та їхня матеріально-технічна база.

Сучасне підприємство – об'єднує в складну систему велику кількість різнорідних компонентів, які в процесі функціонування підприємства можуть модифікуватися. Різноманіття та складність впливу внутрішніх та зовнішніх чинників часто не піддаються чіткому кількісному оцінюванню. Це призводять до того, що ця складна система може набувати нові якості, не властиві її складовим компонентів.