ХМАРНІ ТЕХНОЛОГІЇ: ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРАТАК НА МОРСЬКОМУ СУДНІ

Кравцова Людмила Володимирівна
канд. техн. наук, доцент, доцент кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія Україна

Камінська Наталія Геннадіївна
викладач кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

За визначенням, хмарні технології (cloud computing) – це технології розподіленої обробки цифрових даних, за допомогою яких комп'ютерні ресурси надаються інтернет-користувачу як онлайн-сервіс. При цьому всі необхідні для роботи програмні додатки та їх дані знаходяться на віддаленому інтернет-сервері и тимчасово кешуються на клієнтському боці: його персональному комп'ютері, ноутбуках, комп'ютерному обладнанні та інше.

З точки зору даного дослідження, нас цікавить питання використання хмарних технологій у морській галузі.

Хмарні сервіси забезпечують можливість більш ефективного використання додатків при обробці великих обсягів даних, при цьому значно знижуючи ризики кібернебезпеки [1]. Хмарні обчислення дозволяють узагальнювати інформацію про технічний стан бортового обладнання, окремих систем управління судном, оптимізувати його технічне обслуговування. Але головне, за думкою фахівців, хмарні технології дозволяють підвищити інформаційну безпеку, тобто кібербезпеку суден, що користуються саме хмарними сервісами. Якщо користуватися традиційними методами зберігання інформації в окремих базах даних, кожна з яких має власні вимоги для забезпечення інформаційної безпеки, то це підвищує вразливість взагалі всієї системи. У цьому сенсі переваги переходу до хмарної інфраструктури полягають в тому, що єдині вимоги забезпечують максимальну захищеність. Крім того, хмарні провайдери обмежують несанкційний доступ до даних подвійним шифруванням, та для захисту файлів від прослуховування використовують протокол TLS (англійською: Transport Layer Security). Це означає, що файли, які були завантажені у захищене хмарне сховище, ніяким чином неможливо дешифрувати, оскільки немає ключів шифрування, що практично виключає будь-які зловмисні дії з боку кіберзлочинців.

Але, як показує аналіз джерел, більшість суден транспортної галузі користуються традиційними інтернет-технологіями. Тому статистика кіберзлочинів, пов'язаних з всім, що стосується морських перевезень, дуже сумна. Причин такого стану на морському флоті декілька, починаючи з того що перехід на хмарні сервіси потребує значних фінансових вкладень, та закінчуючи тим, що у міжнародних морських компаній не вистачає фахівців, які б були спроможні працювати з сучасними сервісами на належному рівні. З одного боку, не всі компанії можуть собі дозволити вкладати великі кошти у власну кібербезпеку; з іншого, втрати від кібератак іноді можуть значно перевищувати будь-які витрати на власний захист.

Треба підкреслити, що Міжнародна морська організація (англ.: International Maritime Organization, IMO) до уразливих суднових систем відносить: системи ходового містка; системи обробки і управління вантажем; системи управління

двигунами, машинами і живленням; системи контролю доступу; системи обслуговування і управління пасажирами; публічні інтернет-мережі судна, призначені для використання пасажирами; адміністративні системи та мережі; системи зв'язку. Тобто, будь-яке морське судно є дуже уразливим відносно кібервтручань. Далі, при вивченні цих питань необхідно враховувати фактори мотивації кіберзлочинців, до яких відносять наступні: неправомірне використання кіберпростору (кібер-зловживання); визначені цілі груп активістів; шпигунство; організована злочинність; тероризм; війна. Суб'єкти загрози також групуються за певними ознаками, від звичайних хакерів, до шахрайських кібер корпорацій, здатних нанести непоправну шкоду як окремому судну, так і всій компанії.

Зростання кіберзагроз відносно морської галузі спонукає власників судноплавних компаній звернути прискіпливу увагу на способи рішення цієї проблеми. В останній час, за аналізом фахівців, більшість компаній переходить до сучасних методів кіберзахисту свого флоту, тобто до використання хмарних технологій зберігання суднових баз даних, документації, інформаційного забезпечення управління судновим обладнанням. Але такий перехід потребує відповідно підготовлених спеціалістів, причому, цей спеціаліст має отримати навики роботи у сучасних технологіях у відповідних навчальних закладах. Тобто, це має бути заплановано відповідною навчальною програмою їх підготовки.

Детальне дослідження цього питання привело до деяких висновків, які можна вважати проектом програми підготовки фахівців морської галузі у тій частині, що стосується кібербезпеки судноплавства. Завдяки досвіду роботи у Херсонській державній морській академії, ми розглядаємо вже існуючі курси навчального плану та пропонуємо доповнити його новим курсом, який допоможе стати нашим випускникам-навігаторам максимально конкурентоспроможними на міжнародному ринку праці на морі.

На даний час на першому курсі курсантам-навігаторам викладається дисципліна «Інформаційні технології», метою якої є формування предметних компетентностей, необхідних для ефективного та раціонального використання сучасних інформаційних технологій у майбутній професійній діяльності, формування елементів цифрової грамотності при розв'язуванні задач, пов'язаних з опрацюванням великих обсягів інформації, її пошуком, систематизацією, зберіганням під час експлуатації суднового обладнання. Далі, на другому курсі курсанти вивчають дисципліну «Кібербезпека суднових комп'ютерних систем та мереж». Згідно Кодексу ISM (англ.: International Safety Management), що підтримується Резолюцією IMO MSC.428 (98) [2-3], про забезпечення судновласниками оцінки кіберризиків та вживання відповідних заходів щодо всіх функцій своєї системи управління безпекою, дисципліна знайомить з можливими ризиками, які пов'язані з кібербезпекою судна, та заходами їх усунення, правилами безпечного користування засобами зв'язку, методами захисту від кібератак, сприяє набуттю навиків та вмінь формулювати логічні гіпотези, приймати рішення з усунення проблем кібернебезпеки на підставі аналізу роботи комп'ютерних моделей.

Заключним етапом всебічної підготовки судноводія з питань кібербезпеки має бути впровадження дисципліни, яка викладається на випускному курсі та метою якої є вивчення теоретичних основ хмарних технологій, їх внутрішньої структури та практичної реалізації і прикладних питань їх використання. Попередня назва дисципліни «Управління безпекою судноплавства у хмарних сервісах». Аналіз проблеми привів до висновків, що обсяг дисципліни має складати мінімум 5 кредитів ECTS (150 годин, з них 60 аудиторних), та містити такі розділи:

1. Основні характеристики хмарних технологій, їх відмінність від локальних серверних технологій.

2. Переваги хмарних сховищ інформацій. Ризики, пов'язані з використанням хмарних обчислень.

3. Передумови переходу в хмари. Забезпечення кіберзахисту суднових активів.

4. Огляд хмарних архітектур. Мережеві моделі хмарних сервісів. Сутність та концепції архітектур IaaS, SaaS. Основні PaaS-платформи. Огляд платформ Amazon EC2, Google Apps, Windows Azure. Інші PaaS-платформи.

5. Управління екземплярами додатку. Зберігання даних. Налаштування мережевої взаємодії.

6. Основні питання безпеки у хмарах. Кібербезпека використання суднового обладнання.

Це той мінімальний зміст нової дисципліни, яку, як ми вважаємо, потрібно внести у план підготовки судноводія на випускному курсі, з урахуванням вимог IMO для забезпечення його конкурентоспроможності на міжнародному ринку праці у морській галузі. Треба відмітити, що проект пропонованої програми обговорювався з провідними викладачами академії, які є одночасно діючими капітанами або штурманами. Їх досвід роботи у міжнародних компаніях однозначно підтверджує необхідність впровадження пропонованої дисципліни саме для курсантів випускного курсу.

Список використаних джерел:

1. Mell Peter, Grance Thimothy. «The NIST Définition of Cloud Computing (Draft)» // Recommendations of the National Institute of Standards and Technology, Special Publication 800 - 145 (Draft), September, 2017.
2. Model course 1.25: General operator's certificate for the Global Maritime Distress and Safety System (GMDSS). London: International Maritime Organisation publishing service, 2015. 304 p.
3. Resolution A.703(17) adopted on 6 November 1991. Training of radio personnel in the Global Maritime Distress and Safety System (GMDSS). URL: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.703(17).pdf.