програми і застосовувати відповідні методи і засоби навчання. Відбір і конструювання змісту дисциплін необхідно будувати з урахуванням інтегративних зв'язків, з орієнтованістю на досягнення виділених результатів навчання. Оновлення змісту математичної освти на підставі інтегративного підходу, міждисциплінарна взаємодія математичних та спеціальних інформатичних навчальних дисциплін, координація в часі їх вивчення вирішує центральне питання в підготовці сучасного ІТ-фахівця – покращення якості знань.

Впровадження поняття компетентнісно-інтегративного підхіду спрямоване на якісне вдосконалення існуючих педагогічних систем і обумовлює інноваційний тип діяльності сучасних навчальних закладів. Це сприяє створенню інноваційно-творчої атмосфери взаємодії між учасниками процесу професійної підготовки, формування готовності майбутнього фахівця до реалізації інноваційної діяльності в умовах освітнього простору. При реалізації єдиної стратегії професійної підготовки студентів має бути закладена ідея інтеграції особистісних, соціальних і діяльнісних аспектів, що сприяє координації змісту навчальних дисциплін (зовнішня інтеграція) і формуванню інтегральних характеристик особистості майбутнього фахівця (внутрішня інтеграція).

Отже, впровадження комптентністно-інтегративного підходу в професійну освіту фахівців галузі «Інформаційні технології» суттєво поліпшує якість розуміння спеціальних інформатичних дисциплін, а в наслідку більш ефективно застосовуються отримані знання для вирішення професійних завдань та складних не алгоритмізованих технологічних проблем.

ТИМОФЄЄВА І.Б.,старший викладач кафедри математичних методів та системного аналізу, Маріупольського державного університету

КІБЕРЗАГРОЗИ У ХМАРНИХ ТЕХНОЛОГІЯХ

На сьогоднішній день проблеми виявлення, розслідування та запобігання кіберзлочинам є надзвичайно актуальними. Впровадження сучасних технологій в економіці, управлінні, кредитово-банківській діяльності, стрімкий розвиток інформаційних і телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет зумовило зростання злочинних проявів у різних сферах діяльності людини.

Одним із аспектів розповсюдження широкого діапазону кіберзлочинів, які включають злочини, що здійснюються з метою отримання фінансової вигоди, злочини, пов'язані з використанням інформації, що знаходиться в комп'ютері, а також злочини, направлені проти конфіденційності, цілісності і доступності комп'ютерних систем [3], стає небезпека хмарних технологій.

Термін «хмара» (Cloud) широко використовують для позначення різних технологій та послуг в телекомунікаційній індустрії, як абстрактне позначення мережі в системних діаграмах його застосували вперше, а вже потім в Internet, який в теперішній час відіграє фундаментальну роль у хмарних обчисленнях (Cloud computing), оскільки представляє собою платформу, за допомогою якої сервіси хмарних обчислень стають доступними споживачам [1, с.33].

Згідно з визначенням Національного інституту стандартів і технології (NIST) у США, хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути забезпечені та оперативно надані з мінімальними управлінськими затратами чи зверненням до провайдера послуг. «Хмарою» метафорично називають Інтернет, який приховує всі технічні деталі. Застосовують класифікацію за критерієм надання прав доступу до сервісів та ресурсів адміністративним центром хмари, за яким виділяють чотири типи хмарних обчислень: публічні хмари, які відкриті для широкої публіки; приватні хмари, які розгорнуто на приватному обладнанні та в приватних цілях; гідридні хмари, які є комбінацією двох попередніх типів; суспільні хмари, які характеризуються мульти- адміністративними правами керування, є поєднанням всіх попередніх типів та створюються для дуже специфічних цілей [1, с.36].

В Україні використання систем хмарних обчислень регулюється загальними нормами законів про інформацію та її захист і положеннями приватного права. В свою чергу, у Верховній Раді України 24 березня 2016 року зареєстровано Проект Закону «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень» [2], який має виправити ситуацію із розпоряджанням інформацією.

Із прийняттям вказаного проекту можна говорити про гарантії захисту інформації та забезпечення виконання належним чином обов'язку із її зберігання провайдером шляхом запропонованого у вказаному Проекті переліку чисельних істотних умов, які мають міститись у договорі між надавачем хмарних послуг та володільцем інформації або власником системи. Головними із них є: порядок отримання володільцем інформації або власником системи інформації, яка оброблялась в системі хмарних обчислень, у випадку припинення надання хмарних послуг; порядок видалення інформації із системи хмарних обчислень; відповідальність сторін договору.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом використовуються засоби захисту інформації, які мають сертифікат відповідності чи позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації. Це означає, що для роботи державних інформаційних ресурсів за допомогою хмарних обчислень або для обробки інформації із обмеженим доступом кожному із осередків розміщення інформаційної інфраструктури системи необхідно бути сертифікованим відповідно законодавства України [4].

Існує ряд проблеми, пов'язаних з безпекою хмарних обчислень, але ці питання діляться на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг (організації, які надають програмне забезпечення, платформи, чи інфраструктуру як послуги через використання хмарних технологій) і питання безпеки, з якими стикаються їх клієнтів (компанії або організації, які розгортають додатки або зберігають дані на хмарі) [5]. Відповідальність йде в обох напрямках, тобто: постачальник повинен гарантувати, що їх інфраструктура знаходиться в безпеці і що дані та додатки клієнтів захищені, в той час як користувач повинен вживати заходи, щоб зміцнювати їх застосування, використовувати надійні паролі і перевірку автентичності.

Користувач стає залежним від провайдера хмари та може втратити контроль над інформацією. В такому випадку гостро постає питання порядку витребування інформації у незаконного володільця й відшкодування завданої шкоди за допомогою загальних засобів захисту цивільних прав.

Широке використання віртуалізації в реалізації хмарної інфраструктури спричиняє проблеми безпеки для клієнтів або орендарів публічного хмарного сервісу. Віртуалізація змінює відношення між ОС і базовим обладнанням – будь то обчислення, зберігання чи мережі. Це вносить додатковий шар – віртуалізації – що сам по собі повинен бути правильно налаштований та закріплений. Певні проблеми мають можливе рішення – компромісне програмне забезпечення віртуалізації, або «гіпервізор». У той час як ці проблеми мають здебільшого теоретичний характер, вони все ж існують.

Коли організація вибирає для зберігання даних або розгортання додатків публічному хмарі, вона втрачає можливість мати фізичний доступ до серверів з інформацію. В результаті, конфіденційні дані не зазнають ризику інсайдерських атак. Згідно з недавнім звітом від Cloud Security Alliance, інсайдерські атаки треті за величиною загрози в області хмарних обчислень. Таким чином, постачальники хмарних послуг повинні забезпечити, ретельні перевірки для співробітників, що мають фізичний доступ до серверів в центрі даних. Крім того, центри обробки даних повинні постійно контролювати підозрілу активність.

Для того, щоб зберегти ресурси, скоротити витрати, та зберегти ефективність, провайдери хмарних послуг часто зберігають більше одного разу дані клієнта на тому ж сервері. В результаті, існує ймовірність того, що особисті дані одного користувача можуть бути доступні іншим користувачам (можливо, навіть конкурентам). Для вирішення таких складних ситуаціях, постачальники хмарних послуг повинні забезпечувати правильну ізоляцію даних і логічні сегрегації зберігання [4].

Отже, хмарні обчислення – наступний етап інформаційного розвитку людства. В Україні досі залишається відкритим процес формування нормативно-правової бази врегулювання відносин з приводу їх використання. Досі для появи на теренах нашої держави послуг з надання хмарних сервісів вистачало лише договірного регулювання, однак для їх вдосконалення і подальшого поширення в українське законодавство мають бути внесені зміни з обов'язковим врахуванням розвитку хмарних технологій.

Список використаних джерел

1. Глоба Л. Cloud Computing та його застосування на підприємствах зв'язку / Глоба Л.С., Вольвач Є. О. // СПТЕЛ - 2013 (30 жовтня - 2 листопада 2013 р., м. Львів), 2013. – С. 33-40.
2. Закон України «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень». URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1N268W.html (дата звернення 19.10.2017)
3. Орлов О. Попередження кіберзлочинності–складова частина державної політики в Україні / О.В. Орлов, Ю.М. Онищенко - Теорія та практика державного управління, 2014
4. Хмарні обчислення в правовому полі України. URL: http://jurblog.com.ua/2016/08/hmarni-obchislennya-v-pravovomu-poli-ukrayini/ (дата звернення 19.10.2017)
5. Swamp Computing" a.k.a. Cloud Computing URL: http://security.sys-con.com/node/1231725 (дата звернення 19.10.2017)

ЧУНИЦЬКА В. В., студентка ЗНТУ,
ГАЙТОТА Є. В., студентка ЗНТУ
НІКУЛІЩЕВ Г. І., старший викладач кафедри ЗНТУ

АНАЛІЗ ЗАКОНУ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на одну з ключових арен протиборства. Україна

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
МАРІУПОЛЬСЬКА МІСЬКА РАДА
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В ДОНЕЦЬКІЙ ОБЛАСТІ
ДОНЕЦЬКЕ УПРАВЛІННЯ КІБЕРПОЛІЦІЇ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Збірник матеріалів наукового круглого столу

«КІБЕРБЕЗПЕКА ТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ВИКЛИКИ СЬОГОДЕННЯ»

26 ЖОВТНЯ 2017 РОКУ

Маріуполь – 2017 р.

УДК 004.49(08)
ББК 32.97

Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р. / Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – 104 с.

Рекомендовано до друку засіданням Вченої ради економіко-правового факультету Маріупольського державного університету (протокол № 2 від 18 жовтня 2017 р.)

ЗМІСТ