Байрамов В.Е., студент,
Науковий керівник: ***Лобанчикова Н.М., к.т.н., доц.,***
Житомирський державний технологічний університет

АНАЛІЗ ТЕХНОЛОГІЙ ЗАХИСТУ ХМАРНИХ ОБЧИСЛЕНЬ

Хмарні технології з кожним роком все більше використовуються для задоволення різних потреб населення. І, якщо раніше, хмарні технології використовувалися вузьким колом IT-спеціалістів, то сьогодні дана технологія є доступною для кожного користувача. Використання безкоштовного поштового сервісу gmail компанії Google, Hotmail компанії Microsoft, використання віртуальних дискових просторів, додатків для спільної роботи віддалених користувачів та інші сервіси, що стали звичними для людства. Широке використання хмарних технологій призвело до появи специфічних для кіберпростору та технологій загроз безпеки інформації. Тому досить актуальним є розробка нових інформаційних технологій захисту інформації в кіберпросторі та безпеки хмарних обчислень.

Хмарні обчислення (cloud computing) – це технологія розподіленої обробки даних в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс, тобто робочий майданчик на віддаленому сервері. Терміни «хмарні технології» / «хмарний сервіс», з їх загальноприйнятим графічним представленням, у вигляді «хмарок», тільки плутає користувачів, насправді їх структуру, можна легко зрозуміти, якщо уявити її у вигляді такої піраміди. Основа піраміди «інфраструктура» – це набір фізичних пристроїв (сервери, тверді диски тощо), над нею надбудовується «платформа» – набір послуг і верхівка – програмне забезпечення, що доступне за запитом користувачів. Хмарні обчислення – це певний базис-вектор, отриманий в результаті синтезу цілого ряду технологій і підходів.

За формою власності «хмари» поділяються на публічні, приватні та гібридні. Можливості хмарних обчислень: доступ до особистої інформації з будь-якого комп'ютера, що підключений до Інтернету; можливість працювати з інформацією з різних пристроїв (ПК, планшети, телефони і т.п.); незалежність від операційної системи комп'ютера користувача – веб-сервіси працюють в браузері будь-яких ОС; одну інформацію можна переглядати і редагувати одночасно з різних пристроїв; багато платних програм є безкоштовними (або дешевшими) веб-додатками; запобігання втрати інформації, вона зберігається в хмарних сховищах; завжди актуальна і оновлена інформація; використання останніх версій програм і оновлень; можливість об'єднання інформації з іншими користувачами; легко ділитися інформацією з людьми в будь-якій точці земної кулі.

Недоліки: необхідність постійного з'єднання з Інтернет; програмне забезпечення та його «кастомізація» (є обмеження по ПЗ, яке можна розгортати на «хмарах» і надавати його користувачеві, користувач має обмеження у використовуваному забезпеченні та іноді не має можливості налаштувати його під свої власні цілі); конфіденційність даних, що зберігаються в публічних «хмарах», в даний час, викликає багато суперечок, але в більшості випадків експерти сходяться в тому, що не рекомендується зберігати найбільш цінні для компанії документи на публічній «хмарі», оскільки в даний час немає технології, яка б гарантувала 100% конфіденційність даних; безпека, «хмара» саме по собі є достатньо надійною системою, однак при проникненні в неї зловмисник отримує доступ до величезного сховища даних. Ще один мінус, – це використання систем віртуалізації в яких, як гіпервізор, використовуються ядро стандартних ОС (наприклад Windows), що дозволяє використовувати віруси та вразливості системи; для побудови власної хмари необхідно виділити значні матеріальні ресурси, що не вигідно щойно створеним і малим компаніям; подальша монетизація ресурсу.

Напрямками захисту є створення нових інформаційних технологій: управління ідентифікацією користувачів з використанням комбінації сучасних методів аутентифікації; фізичного захисту IT-обладнання (серверів, маршрутизаторів, кабелі і т. д.) від несанкціонованого доступу, крадіжки перешкод, пожеж, повеней і т.д. шляхом використання комплексних систем захисту; мінімізація можливості відмови в роботі сервісів шляхом резервування та безперебійної подачі електроенергії; нові підходи до підбору персоналу (безпека відбору потенційних новобранців, питання безпеки та навчальних програм, проактивного моніторингу безпеки та нагляду, дисциплінарних процедур і договірні зобов'язання, включені в трудових договорах, угодах про рівень обслуговування, кодекси поведінки, політика тощо); підвищення доступності хмарних сервісів шляхом реплікацій, резервування, перенаправлення, повнозв'язкових топологій; забезпечення належної безпеки додатків шляхом підвищення стійкості додатків до шкідливого програмного забезпечення; підвищення захищеності персональних даних шляхом комбінування методів криптографічних перетворень та методів аутентифікації користувачів; удосконалення алгоритмів шифрування з метою підвищення їх криптостійкості шляхом комбінування відомих методів.