УДК 004. 056

В.Ю. КОРОЛЬОВ

ЗАХИСТ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ USB-ФЛЕШ НАКОПИЧУВАЧАХ ДЛЯ ХМАРНИХ ОБЧИСЛЕНЬ

Анотація. *Розглянута проблема комп'ютерної безпеки використання флеш накопичувачів у складі хмарної архітектури сучасних організацій. Побудовано схему інформаційних потоків DFD з границями довіри взаємодії накопичувача з корпоративною мережею та проведено оцінку комп'ютерної безпеки за методиками STRIDE і DREAD.*
Ключові слова: *хмарні обчислення, безпека, флеш накопичувачі, STRIDE, DREAD.*

Аннотация. *Рассмотрена проблема компьютерной безопасности использования флеш накопителей в составе облачной архитектуры современных организаций. Построена схема информационных потоков DFD с границами доверия взаимодействия с компьютерной сетью корпорации и проведена оценка компьютерной безопасности по методикам STRIDE и DREAD.*
Ключевые слова: *облачные вычисления, безопасность, флеш накопители, STRIDE, DREAD.*

Abstract. *The problem of computer security with using flash-stick in composition of cloud computing is discussed. The Data Flow Diagram with trust boundaries of interaction corporate net is presented. The Threat Tree and STRIDE and DREAD evaluation of computer security are given.*
Keywords: *cloud computing, security, flash drive, STRIDE, DREAD.*

1. Вступ

Зростання обчислювальних потужностей серверних ферм, об'ємів пам'яті датацентрів та пропускної здатності Інтернет-каналів обумовлює перехід до хмарних обчислень, які дозволяють дистанційно користуватись віртуалізованою комп'ютерною інфраструктурою як послугою. Подібні перетворення почалися на початку XX століття [1], коли крупні виробники товарів і продуктів стали закуповувати електроенергію як послугу замість побудови власних електростанцій. Подібно до цього, сьогодні фірми-виробники програмного забезпечення трансформуються у постачальників послуг, які акумулюють великі обчислювальні потужності і розподілені сховища даних великих об'ємів пам'яті, що пропонуються кінцевому споживачу. Поступово також змінюється програмне забезпечення (ПЗ) і для пересічних користувачів персональних обчислювально-телекомунікаційних засобів, що ставить нові задачі в області комп'ютерної безпеки і захисту конфіденційної інформації.

Основна частина. З точки зору економіки, впровадження хмарних обчислень дозволяє зменшити вартість володіння серверною інфраструктурою та пов'язану з нею капіталізацію бізнесу за рахунок переносу величини витрат у бік операційних витрат: за оренду віртуалізованих хмарних обчислювальних ресурсів і датацентрів та їх обслуговування. Також початкові витрати для початку бізнесу з використанням публічних хмар значно менші, ніж закупівля власних серверів і приміщень, та суттєво менші при оренді обчислювальних потужностей і обслуговування обчислювальної інфраструктури типу хостинг [2].

Постановка задачі. Слід відмітити, що все більша частина працівників використовує приватну власну особисту обчислювальну техніку для вирішення бізнес-задач (consumisation) завдяки чому відбувається взаємопроникнення корпоративних та споживацьких інформаційних технологій, сервісів та задач. Прикладами переходу сервісів у хмари є офісні продукти, антивірусне ПЗ, сервіси зберігання і конвертації мультимедійних файлів та ін. Все більше на ринку пропонується веб-сервісів для смартфонів та планшетних ПК з доступом до мережі Інтернет, які базуються на хмарній обчислювальній платформі, що одночасно потребує вирішення науково-прикладних спільних задач підвищення комп'ютерної безпеки та розв'язання нових задач захисту інформаційних технологій кор-

поративного та індивідуального використання [3]. Тому підвищення захисту мобільних пристроїв зберігання, які використовуються як локально, так і в обчислювальних хмарах, є актуальною науковою проблемою.

Аналіз останніх досліджень і публікацій. Відомо, що більша частина часу навантаження процесорів, навіть віртуалізованих корпоративних серверів, не перевищує 50-70%. Навпаки, в періоди пікових навантажень наявних обчислювальних потужностей не достатньо і швидко їх збільшити фізично і організаційно неможливо. На противагу для публічної хмарної інфраструктури така проблема вирішується простим запитом нових ресурсів. З технічної точки зору, перехід до хмарної інфраструктури означає перенос віртуалізованої частини обчислювальних ресурсів корпорації за межі її фізичного периметра та брандмауера, що потребує розробки нових технологій та протоколів безпеки [3, 4].

2. Сервісно-орієнтована архітектура як база для хмарних обчислень

Хмарні обчислення є подальшим розвитком сервісно-орієнтованої архітектури і технологій віртуалізації у глобальному масштабі. Концепція сервісно-орієнтованих архітектур (СОА) і відповідне програмне забезпечення розвиваються вже понад десять років. На думку більшості фахівців, найкраще означення СОА таке [5]. СОА – це каркас для інтеграції бізнес-процесів з IT-інфраструктурами у формі безпечних, стандартизованих служб-компонентів, що можуть використовуватись багаторазово і комбінуватися з іншими для швидкої адаптації у відповідності з поточними пріоритетами організації. Типова СОА складається з чотирьох основних доменів високого рівня: сервіси, інфраструктурні служби, прикладні служби та сервісна шина підприємства.

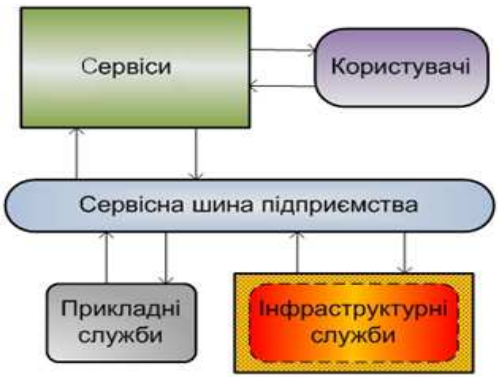

Рис. 1. СОА інформаційних технологій організації

У відповідності з концепцією СОА структура служб має вигляд, представлений на рис. 1.

Користувачами можуть бути співробітники корпорації, що працюють в головному офісі або поза його межами, які підключені до СОА через Інтранет або Інтернет, партнери або споживачі послуг та товарів, які виробляє організація, що підключена до СОА через Інтернет.

У контексті СОА акцент комп'ютерної безпеки зміщується у сторону захисту архітектури. З одного боку, необхідно лишити сервіси – будівельні блоки СОА відкритими настільки, щоб зовнішні і внутрішні додатки могли легко отримувати доступ один до одного для повторного використання будівельних блоків. З іншого боку, якщо ці сервіси не захищені відповідним чином, то вони можуть бути використані зловмисниками для того, щоб організувати витік інформації з організації.

3. Декларативна технологія створення сервісів безпеки

Вирішення проблем безпеки СОА ґрунтується на технології декларативного програмування, яка дозволяє збільшити продуктивність розробки додатків і підвищити функціональну гнучкість сервісів [5]. Переваги декларативного програмування для безпеки СОА головним чином стосуються підвищення ефективності паралельного використання професійних знань фахівців у предметних галузях і програмістів при їх спільній роботи над проектами. Отже, експерти в області безпеки декларативно визначають політики безпеки, а розробники можуть втілювати ці політики без потреби у тісній співпраці з експертами.

4. Безпека сервісів у контексті СОА

На рис. 2 показано три додатки: два на серверах головної компанії і один на сервері організації-партнера. Видно, що чотири клієнтських додатки можуть використовувати будь-які послуги з трьох згаданих серверних додатків та обмінюватись повідомленнями. Зрозуміло, що жоден з додатків не має повного опису системи комп'ютерної безпеки для всіх випадків, ситуацій і контекстів. Додаткам потрібні мінімальні відомості про систему комп'ютерної безпеки для того, щоб, наприклад, знати, як викликати сервіс безпеки або як використовувати дані, надані сервісом безпеки. Отже, суть логіки безпеки повинна виконуватись центральним сервісом безпеки.

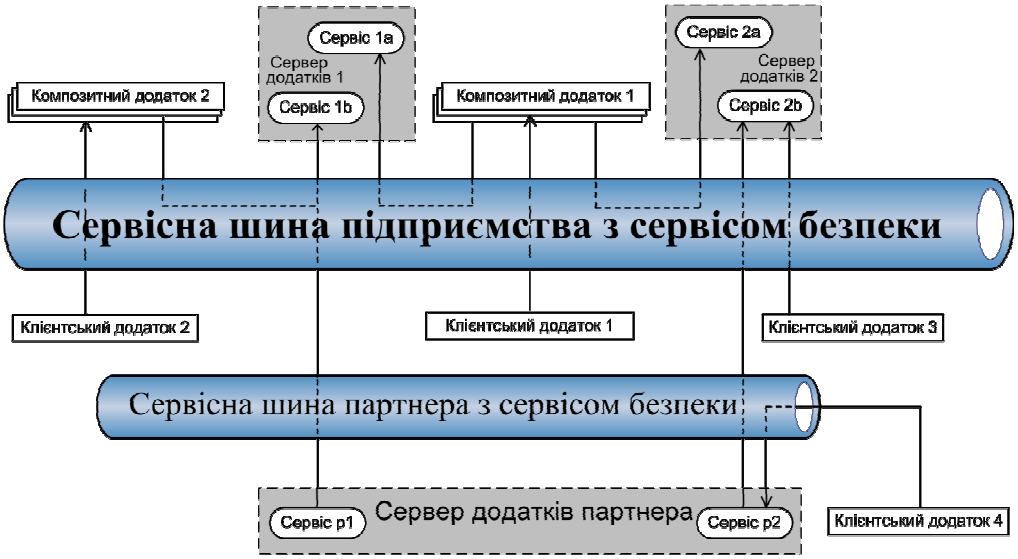

Рис. 2. Модель СОА, де безпека впроваджена як інфраструктурний сервіс, вбудований у сервісну шину підприємства

При такому підході відсутні проблеми, що виникають при поєднанні додатків та сервісів з різними моделями безпеки. Ці сервіси безпеки подібні до прикладних сервісів, проте мають свою специфіку, оскільки є інфраструктурними сервісами і можуть виконувати свої функції, навіть якщо їх безпосередньо не викликають.

Наприклад, сервіс безпеки може бути впроваджено в інформаційну інфраструктуру організації як частину сервісної шини або за допомогою апаратних мережевих пристроїв з інтегрованими інтелектуальними додатками. Оскільки сервіс безпеки є центральним і не є частиною жодного додатку, його модель може розвиватись разом з бізнес-вимогами без впливу будь-яких додатків. Поводження з безпекою, як з сервісами, допомагає розвантажити розробників сервісів від питань захисту інформації та дозволяє зосередитись на логіці додатків.

5. Комп’ютерна безпека в контексті використання флеш накопичувачів і взаємодія СОА з портативними програмними додатками

Рівень інформаційної та фізичної безпеки персональних накопичувачів інформації працівників великих корпорацій, діяльність яких пов’язана з високими технологіями або фінансами, службовців державних установ, які працюють з інформацією обмеженого доступу, офіцерів військових структур тощо повинна забезпечувати захист від технічно високооснащеного супротивника на рівні іноземної спецслужби або міжнародного злочинного хакерского угрупування. Тому до таких накопичувачів висуваються підвищені вимоги до реалізації криптографічних систем захисту інформації, а продукти, які пройшли сертифіка-

цію, часто заборонені до експорту та обмежені списком країн-партнерів США або лояльних держав.

Постановка завдання. Природним рішенням у контексті хмарних обчислень є додавання у сервісну шину хмари інфраструктурного сервісу, що взаємодіє з мобільними пристроями, до яких відносяться флеш накопичувачі [6–12]. Взаємодія корпоративної інформаційної системи з інфраструктурним сервісом мобільних пристроїв виконується через сервіс безпеки. Підтримка такого рішення найбільш повно реалізується сервісом безпеки Security as Service та набором програм комп'ютерної безпеки [3, 5]. Впровадження хмарних обчислень загострює питання надійності автентифікації користувачів та розмежування прав доступу, оскільки інформація з обмеженим доступом знаходиться поза територією фірми, тому організаційні та фізичні методи керування безпекою не можуть бути використані повною мірою для компенсації загроз несанкціонованого доступу.

Виклад основного матеріалу. Необхідність використання апаратних засобів для забезпечення ефективного захисту інформації обумовлена тим, що програмні рішення можуть захистити лише від прочитання викраденої інформації, а сам процес передачі даних флеш накопичувачем при підключенні до ПК – ні. Крім того, високорівневі програмні рішення можуть бути вимкнені або модифіковані зловмисними програмами, що використовують уразливі особливості Windows ОС.

Прикладом ПЗ, безпеку якого складно контролювати, є технологія відкритих та закритих зон пам'яті мобільних пристроїв зберігання. Ця технологія застосовується також для корпоративних флеш накопичувачів, які використовуються для роботи і в особистих цілях. Оскільки у світі набирає актуальності тенденція повної або часткової домашньої роботи з гнучким графіком зайнятості, а також багато службовців працюють у відрядженнях, тому такі продукти мають свою нішу і продовжують випускатись.

Для ОС Windows флеш накопичувач з відкритою і закритою зонами є віртуальним емульованим CD-приводом з ПЗ і зовнішнім диском, в пам'яті якого зберігатимуться файли. З точки зору безпеки, наявність відкритої і закритої зон ускладнює керування безпекою інформації. Команди на доступ до відкритих і закритих сегментів пам'яті подаються контролером пристрою зберігання за допомогою високорівневих функцій-сервісів і драйверів ОС, з яких на флеш накопичувач повинна проходити команда на розблокування доступу. За допомогою зловмисних програм команди можливо перехопити або підмінити [13]. Тому в найбільш захищених корпоративних флеш накопичувачах використовуються тільки закриті зони. В одній зоні зберігаються сервіси безпеки та офісне високорівневе пПЗ [7, 11] (портативне програмне забезпечення призначене для запуску з накопичувача без інсталяції в ОС) і ПЗ, яке оновлюється за командою системного адміністратора фірми, друга закрита зона використовується тільки для даних.

У табл. 1 наведено основні характеристики USB-флеш накопичувачів, які пропонують розробники для експлуатації у корпоративних, державних та військових організаціях. Видно, що середня вартість флеш накопичувачів приблизно складає 160 дол. США, з чого можна зробити висновок, що розробка таких виробів є складною технічною задачею, вироби потребують високоякісних мікросхем та проходять сертифікацію. Вибір продуктів обмежено форматом звичних ручних флешок, які є найбільш поширеними у практиці.

Оскільки об'єм статті є обмеженим, далі представлено скорочений огляд характеристик сучасних корпоративних накопичувачів. Розглядаються тільки найкращі зразки з запропонованих фірмою з найповнішим набором програм для комп'ютерної безпеки та загальні тенденції їх використання протягом найближчих трьох років.

Сертифікація не гарантує захищеності від зламу корпоративних накопичувачів, які трапляються [13], а означає, що криптографічні функції та фізичний захист пристрою реалізовані у відповідності до документів Національного інституту стандартів США. Сертифікація FIPS 140-2 стандартизує розробку пристроїв з криптографічними модулями. Цей

стандарт запроваджено і у Канаді. Вимоги до рівня захисту інформації регулярно переглядаються й підвищуються. Так, у FIPS 140-2 lev. 3 підвищено вимоги до фізичного захисту і сигналізації щодо зламу корпуса накопичувача. Вже оприлюднено FIPS-140-2 lev. 4 та закінчується розробка нового стандарту FIPS 140-3. З 2010 сертифіковані накопичувачі використовують оновлені набори криптографічних функцій Suite B, де запроваджено асиметричні алгоритми обміну ключами на базі еліптичних кривих, та багатофакторну автентифікацію.

Таблиця 1. Характеристики USB-флеш накопичувачів корпоративного класу різних виробників

Фірма-виробник	Основний тип автентифікації	Рівень FIPS 140-2	Адміністрування	Наявність антивірусу	Об'єм пам'яті, ГБ	Швидкість читання/ запису, МБ/с	Вартість, дол. США
IronKey	КП	3	+	-	1-32	27|24; 25|17	59-299
Imation	ВП	3	+	+	2-64	17|6	129-683
SpyRus	КП	3	+	+	(2-32)	20|10	200-236
Lok-it	PIN-код	3	-	-	4-16	н/д	97-183
Lexar	КП	3	+	+	2-8	30|22	100-270
Gemalto	КП	3	+	+	4	н/д	121
Kanguru	КП	2	+	+	1-128	30|12	40-500
Verbatim	КП	2	+	-	1-8	24|20	118-460
Check Point	КП	2	+	+	4,8	н/д	160, 165
McAfee	ВП |КП	2,3	+	+	1-8	24|20	169-417
Kingston	КП	2	-	-	2-16	18|10	80-212
Sandisk Enteprise	КП	2	+	-	1-8	24|20	58-375
Integral memory	КП	2	-	-	2-32	н/д	67-206
Elytra	КП	2	-	-	1-8	24|20	89-358

КП – введення паролю з клавіатури, ВП – сканування відбитка пальця.

З наведених даних та попередніх робіт [6–12] можна виділити основні показники, за якими флеш накопичувач може бути віднесений до системи з підвищеним ступенем захисту, де реалізовані шифрування потоку даних між комп'ютером та накопичувачем за стандартом AES-256 контролером накопичувача; система обмеженої кількості спроб введення паролю (3-10/20); разові паролі RSASecureID; вмикання на корпусі або при автентифікації режиму пам'яті тільки на читання або читання/запис файлів; система керування ключами на базі асиметричного шифрування та підтримка роботи в режимі багатофакторного автентифікатора.

Провідні виробники також додають високорівневе ПЗ та пПЗ: проактивну систему захисту від шкідливого ПЗ, антивірус або захист від зловмисного ПЗ, менеджер паролів, безпечно сконфігуровані: браузер, поштову програму, сервіс резервного копіювання тощо. Сервісне ПЗ від виробника використовується для підтримки керування життєвим циклом накопичувача, дистанційної зміни паролю та анулювання права доступу у разі його втрати. Слід зазначити, що всі перелічені додаткові сервісні програми можуть бути укомплектовані незалежними системними інтеграторами в залежності від потреб замовника. Водночас найбільш повну комплектацію високорівневими програмами захисту інформації мають накопичувачі, які виходять під торговою маркою McAffeeEnterprise.

Багато виробників запам'ятовуючих пристроїв мають у лінійці продуктів накопичувачів з функціями шифрування потоку даних (на контролері) без сертифікації. До таких фірм відносяться: Aleratec, CryptoKey, EdgeTechCorp, Corsair, BlockMasterSecurity, PatriotMemory, Twinmos, Supertalent, Buffalo, Transcend, HP, Centon та ін. Тобто такі пристрої стали достатньо поширеними з давно відомими криптографічними функціями на ПЛІС (програмовані логічні інтегральні схеми) або на спеціально розробленому чіпі, закупленому фірмою у ліцензованих виробників ядер комп'ютерних пристроїв захисту інформації. Слід зазначити, що для використання сертифікованих флеш накопичувачів з підвищеним рівнем захисту у державних і військових структурах США обов'язкою є вимога, щоб усі компоненти були вироблені у США.

6. Інноваційні рішення провідних виробників корпоративних накопичувачів

Зрозуміло, що корисні інноваційні технічні рішення для комп'ютерної безпеки, винайдені однією фірмою, протягом року впроваджуються усіма учасниками ринку, проте за якістю реалізації окремих технологій вже є і незаперечні лідери.

IronKey однією з перших компаній почала просувати системи захисту інформації від несанкціонованого доступу військового ґатунку для корпоративного, фінансового та урядового сегментів ринку. Вироби фірми IronKey (табл. 1) розглядаються в Інтернет-публікаціях як еталон створення продуктів корпоративних флеш накопичувачів, виробництво яких є її виключною спеціалізацією. Зауважимо, що вироби IronKey ще не вдавалось зламати [13]. Накопичувачі IronKey підтримують роботу в режимі автентифікатора для фінансових, державних і військових установ. Хоча фірмою IronKey реалізовано разові паролі RSASecureID, віртуальну клавіатуру з мікшером та проактивним захистом від перехоплення паролю, проте компанія Lok-it.net у своїй презентації показала, що такі технології не компенсують загрозу перехоплення пароля при введенні його з клавіатури у ОС Windows. Отже, така автентифікація користувачів є ненадійною.

Нова лінійка продуктів для комп'ютерної безпеки фірми Imation стала результатом придбання фірми MxiSecurity. Серед інновацій можна виділити трифакторну автентифікацію: біометрична протяжним сканером відбитка пальця, парольна з клавіатури, CAS|PIV {Common Access Card; Person Identity Veryfication} (спеціалізована мікросхема системи автентифікації в державних і військових установах США); режим декількох користувачів (до 10 користувачів)

Фірма SpyRus випускає широкий спектр продуктів для апаратно-програмного захисту інформації. Для нашого розгляду цікавим є USB-картрідер з криптографічним пристроєм розміром з USB-флеш із зовнішнім підключенням карток флеш-пам'яті до блоку шифрування. У виробах фірми SpyRus підтримується багатооператорний режим використання пам'яті флеш на базі власної шифрованої дискової операційної системи. Використання PKI – системи розподілення ключів дозволило зберігати на сервері найбільш вразливі секретні дані: ключі шифрування, хеш-функції паролів; у флеш-пам'яті пристрою зберігаються тільки зашифровані файли, кожен з яких шифрується окремим ключем.

Lok-it використовує PIN-код для автентифікації власника флеш накопичувача. Принциповою відмінністю рішення Lok-it є набір PIN-коду з кнопок на корпусі флешки для підключення накопичувача до ПК. Після набору правильного коду накопичувач видає користувачу відповідну кольорову індикацію, і власник має 30 секунд для підключення флешки до USB-порту.

McAfee є одним з лідерів виробництва антивірусних програм та систем захисту інформації від несанкціонованого доступу. Ця фірма реалізувала повний спектр високорівневих хмарних сервісів безпеки для флеш накопичувачів корпоративного класу і використовує накопичувачі відомих виробників Imation, Kingston, SanDisk з власними програмними сервісами під своєю торговою маркою. Подібним є рішення і від іншого відомого виро-

бника програмних систем захисту інформації CheckPoint, який реалізував віртуальне офісне середовище з VPN-доступом.

7. Генерація випадкових біт для задач криптографії в контексті флеш накопичувачів

У цілому, як криптографічні функції і протоколи є достатньо формалізованими та стандартизованими, так само стандартизовані вимоги до генераторів дійсно випадкових чисел. Докладний огляд проблеми генерації випадкових чисел для задач криптографії наведено у роботах [12, 14]. У стандартах США та Канади використовують термін "генератор випадкових біт" для криптографії, а не чисел, для того, щоб підкреслити відмінність між задачами генерації псевдовипадкових десяткових чисел для чисельних методів прикладної математики та двійкових чисел для задач шифрування і обміну секретними ключами, для перевірки якості реалізації яких використовують відмінні протоколи та підходи. Стандарт ANSI X9.31 описує вимоги до генераторів випадкових послідовностей біт, що регламентує використання алгоритмів AES 256 або 3DES у програмах криптографічних модулів. Початкові значення для генератора отримують з моніторингу та запису параметрів роботи мікроконтролера. Багато виробників USB-флеш накопичувачів використовують ПЛІС-контролери, тому можливі варіанти побудови генератора випадкових біт на основі кільцевих осциляторів (ring oscillator) в режимі стохастичних коливань як джерела ентропії для криптографічних генераторів випадкових біт [14], які досить просто технічно реалізувати на ПЛІС.

Потреби у збільшенні швидкості передачі даних обумовили введення нового стандарту USB 3.0, яким буде замінено сучасний USB 2.0. На ринку представлено багато виробників дискретних USB 3.0 контролерів: NEC, Intel, Texas Instruments, Via Labs, Mitsubishi Electric, Renesas Electronics, Sypress Semiconductor, ASMedia Technology, Ethron Technology, Fresko Logic та ін. Вже зараз випускаються FIPS 140-2, сертифіковані НЖД з підключенням USB 3.0 з максимальною швидкістю (Buffalo) 4,8 Гбіт/с і є несертифіковані USB 3.0 флеш накопичувачі з шифрування. З технічної точки зору, їх відмінність від USB 2.0 полягає у використанні багатоканальної пам’яті на базі RAID-масивів флеш-мікросхем та DRAM-кешу. Флеш накопичувачі поступово отримують всі технології SSD-дисків: RAID, DRAM-кеш, багатоканальну пам’ять. Тому генератори випадкових біт, джерело ентропії яких грунтується на реєстрації фізичних шумових процесів, повинні комбінуватись з даними, отриманими з запису процесів мікросхем, для досягнення потрібної продуктивності без втрати принципово важливої властивості – непередбачуваності значень чисельної послідовності [12, 14].

8. Моделювання загроз для мобільних носіїв інформації у хмарі

Моделювання загроз для інформаційної системи представляє собою ітеративний процес [15]. В інженерній практиці на основі моделювання загроз створюється документ, за яким команда розробників апаратно-програмних засобів виробляє стратегію комп’ютерної безпеки кінцевого продукту. Переважна більшість відомих успішних атак на комп’ютерні системи мала кінцевою метою кражу інформації з обмеженим доступом. Тому аналіз загроз несанкціонованого доступу до конфіденційної інформації, яка зберігається в обчислювальній хмарі, можна розпочати з побудови діаграми інформаційних потоків з межами довіри (Data Flow Diagram with Trust Boundaries) та дерева загроз (рис. 4). Багато в чому правильна побудова дерева загроз вирішує питання контрзаходів для викликів з боку супротивника. На рис. 3 представлено діаграму інформаційних потоків для флеш накопичувача, підключеного до корпоративної мережі та публічної хмари. Границі довіри на рисунку показано штриховими дугами, процеси-колами, мультипроцеси – концентричними колами, а сутності – прямокутниками. Цей метод у сукупності з подальшими STRIDE і DREAD методи-

ками оцінок уразливостей комп'ютерної безпеки широко використовується компанією Майкрософт у системі SDL+C [6] постановки продуктів на виробництво.

Видно, що дерево загроз подібне до відповідного дерева загроз несанкціонованого доступу до персонального комп'ютера або ноутбука. Основні загрози при роботі накопичувача у корпоративному і позакорпоративному середовищі такі:

I. Несанкціонований доступ до конфіденційної інформації на накопичувачі в результаті його кражі та фізичного зламу.

II. Доступ до інформації з обмеженим доступом, що зберігається у сховищах хмари (документи, електронна пошта).

III. Перехоплення пароля та ключів автентифікації при підключенні до зараженого корпоративного або власного комп'ютера.

IV. Зміна даних облікового запису на сервері та проникнення в інформаційну систему, розміщену на хмарі.

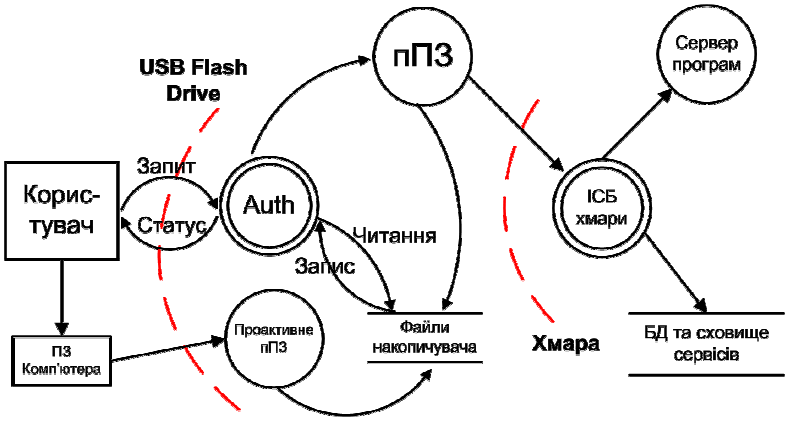

Рис. 3. Діаграма інформаційних потоків для флеш накопичувача корпоративного призначення (Auth – процес автентифікації, ІСБ – інфраструктурний сервіс безпеки) та його взаємодії з ІСБ хмари

Ризик здійснення загрози трактується як добуток імовірності здійснення загрози на величину потенційних втрат. Виявлення загроз та присвоєння їм рейтингу здійснюється на основі методик експертних оцінок DREAD та STRIDE. Розглянемо STRIDE і DREAD оцінки комп'ютерної безпеки, які дозволяють дати якісні і кількісні оцінки величини ступеня загрози комп'ютерній безпеці за розробленими показниками.

На основі рис. 3 можна запропонувати таке дерево загроз.

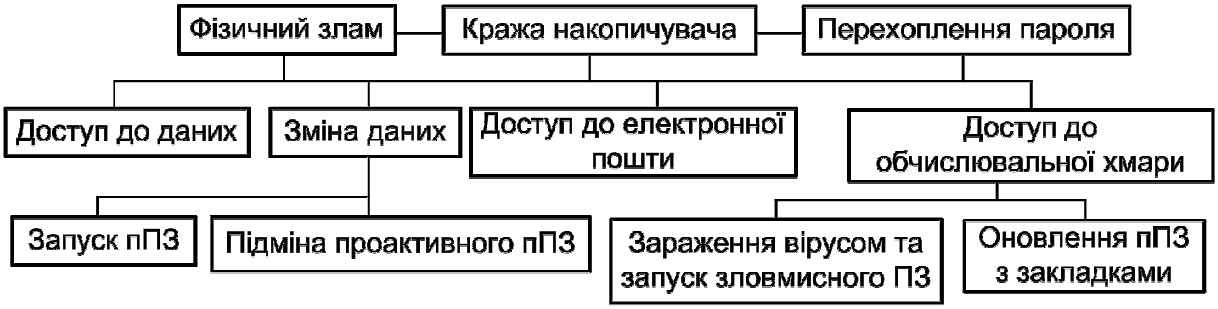

Рис. 4. Дерево загроз для корпоративних флеш накопичувачів

STRIDE-методика якісної оцінки вразливості. STRIDE дозволяє типізувати загрози за цілями і задачами. За STRIDE-методикою експерт оцінює можливість шести основних атак (відображених на дереві загроз уразливостей) за допомогою діаграм інформаційних потоків, процесів, сутностей та файлів за двозначною логікою. Отриманий перелік атак з експертизою можливісті їх проведення дозволяє перейти до розробки стратегії їх протидії.

Перелік атак такий: Spoofing Identity отримання доступу обманним шляхом представлення себе як автентифікованого користувача; Tampering with data підробка даних, тобто супротивник видаляє або модифікує дані; Repudiation, це відмова від факту виконан-

ня дій, означає, наскільки супротивник може виконати атаку без виявлення його слідів та доказів у системі; Information disclosure, означає розкриття інформації, коли атакуючий з низьким рівнем доступу отримує доступ до інформації поза його рівнем допуску; Denial of Service, це відмова обслуговування, атака робить систему недоступною для інших користувачів, наприклад, внаслідок подачі команди на вимикання серверу; Elevation of Privilege, тобто перевищення прав доступу, метою такої атаки є отримання секретних даних, з якими автентифікується користувач з більш високим рівнем доступу. Отримані результати зводяться в таблицю STRIDE (табл. 2).

DREAD-методика оцінки ваги ризиків. Проблема з рейтинговими системами оцінки загроз полягає в тому, що команді важко дійти згоди у призначенні пріоритету загрозам. Тому було запропоновано методику обчислення значимості ризиків. DREAD-методика дозволяє отримати кількісну оцінку значимості загрози на основі опитування експертів, які ставлять бали рівню загроз таким характеристикам атаки: D – Damage potential, це потенційні втрати при успішній атаці; R – Reproductively, характеризує ступінь складності виконання або повторення атаки; E – Exploitability, визначає рівень підготовки супротивника і ресурси, необхідні для успішного виконання атаки; A – Affected users, тобто кількість користувачів, яким буде нанесено збитки при успіху атаки; D – Discoverability, що визначає, наскільки просто атака може бути виявлена і простежений атакуючий. Отримані результати зводяться у таблицю DREAD і всереднюються (табл. 2).

Таблиця 2. Якісна оцінка загроз за методикою STRIDE і оцінка ваги загроз за методикою DREAD

Загроза	S	T	R	I	D	E
I	x			x	x	
II	x	x	x	x		
III	x	x	x			x
IV	x	x		x	x	x

Загроза	D	R	E	A	D	∑/5
I	4	4	4	2	3	3
II	4	4	3	3	3	4
III	3	3	4	2	2	3
IV	4	4	3	3	2	3

Дані, наведені в табл. 2, були заповнені на основі експертних оцінок фахівців з комп'ютерної безпеки відділу 180 Інституту кібернетики ім. В.М. Глушкова НАНУ. На основі запропонованого аналізу комп'ютерної безпеки флеш накопичувачів можна зробити висновок, що для флеш накопичувачів першочерговим завданням є захищення процесу автентифікації користувача та проактивні дії по виявленню атак на віртуалізовану корпоративну мережу у хмарі.

Зрозуміло, що уникнення всіх ризиків і вразливостей навіть за умови їх повної ідентифікації може виявитись складною задачею або потребуватиме залучення значних людських ресурсів, а в деяких випадках вимагатиме повного перероблення проекту системи. В таких випадках замовник системи повинен використовувати економічні чинники при виборі показників захищеності обчислювальної системи.

9. Висновки

Представлено опис архітектури системи безпеки для хмарних обчислень та показані відмінності від класичної клієнт-серверної архітектури: декларативне формулювання політик комп'ютерної безпеки, введення сервісу безпеки хмари в інфраструктуру шини безпеки сервісно-орієнтованої архітектури, збільшення ролі захисту інформації від несанкціонованого доступу і автентифікації користувачів при виконанні всіх операцій.

Наведено тенденції розвитку сучасних USB-флеш накопичувачів корпоративного класу та показано способи їх взаємодії з сервісом безпеки хмар. Побудовано модель комп'ютерної безпеки використання флеш накопичувача у публічній хмарі: дерево загроз та діаграму інформаційних потоків з межами довіри обчислювальних ресурсів у процесі взаємодії хмари з накопичувачем, які показують, що найбільш вразливим є процес автен-

тифікації користувача за допомогою клавіатурних методів. Виконано аналіз безпеки ПЗ на основі методик STRIDE і DREAD, які використовуються фірмою Майкрософт.

СПИСОК ЛІТЕРАТУРИ

1. Carr N. The Big Switch / Carr N. – London: Norton & Company, 2008. – 145 p.
2. Mateos A. The Cloud at Your Service / Mateos A. – Greenwich: Manning Publications, 2011. – 273 p.
3. Mather T. Cloud Security and Privacy / Mather T., Kumaraswamy S., Latif S. – Sebastopol: O'Reilly, 2009. – 335 p.
4. Linthicum D. Cloud Computing and SOA Convergence in Your Enterprise / Linthicum D. – Boston: Addison-Wesley, 2010. – 265 p.
5. Kanneganti R. SOA Security / R. Kannganti, P. Chodavarapu. – Westampton: Manning Publications, 2008. – 511 p.
6. Корольов В.Ю. Концепція побудови персоналізованих флеш накопичувачів даних з апаратним захистом інформації / В.Ю. Корольов, В.В. Поліновський // Математичні машини і системи. – 2009. – № 4. – С. 96 – 105.
7. Королёв В.Ю. Синтез портабельных информационных сервисов для флеш накопителей / В.Ю. Королёв, В.В. Полиновский // Управляющие системы и машины. – 2008. – № 6. – С. 28 – 33.
8. Королёв В.Ю. Стеганография по методу наименее значимого бита на базе персонализированных флеш накопителей / В.Ю. Королёв, В.В. Полиновский, В.А. Герасименко // Управляющие системы и машины. – 2011. – № 1 (231). – С. 79 – 87.
9. Корольов В.Ю. Стан проблеми комп'ютерної безпеки з використанням USB-флеш накопичувачів у державних установах і корпораціях / В.Ю. Корольов // Вісник університету "Україна". – (Серія "Інформатика, обчислювальна техніка та кібернетика"). – 2010. – № 8. – С. 160 – 166.
10. Корольов В.Ю. Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора / В.Ю. Корольов, В.В. Поліновський, О.В. Малікова // Вісник Хмельницького національного університету. – 2008. – № 3. – С. 175 – 181.
11. Корольов В.Ю. Тенденції розвитку портабельних програмних систем / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко // Вісник Хмельницького національного університету. – 2009. – № 1. – С. 233 – 241.
12. Корольов В.Ю. Криптогенератор з використанням перетворення шумів слабострумних електронних кіл / В.Ю. Корольов, В.В. Поліновський // Вісник Черкаського державного університету. – (Серія «Технічні науки. Інформаційні технології, обчислювальна техніка і автоматика»). – 2009. – № 2. – С. 14 – 18.
13. http://www.schneier.com/blog/archives/2010/01/fips_140-2_leve.html.
14. Koc C. Cryptographic Engineering / Koc C. – New York: Springer, 2009. – 528 p.
15. Dowd M. The Art of Software Security Assessment / Dowd M., McDonald J., Schuh J. – San Francisco: Addison-Wesley, 2006. – 1200 p.

Стаття надійшла до редакції 01.09.2011