АНАЛІЗ СУЧАСНИХ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Левкін А.В., канд. техн. наук, доц.
Котко Я.М., канд. техн. наук, доц.
Левкін Д.А., канд. техн. наук, доц.
Державний біотехнологічний університет

Зі стрімким розвитком інформаційних технологій і застосуванням програмно-апаратних засобів в усі сфери життя людини постає питання в гарантуванні інформаційної безпеки. Окрім розвитку засобів збереження і передачі великих об'ємів інформації набули актуальності питання її захисту. Розширення ринку попиту на програмні продукти і засоби телекомунікацій стало поштовхом для модернізації вже існуючих та проектування новітніх програмних продуктів і засобів інформаційної безпеки. Модернізують вже існуючі і проектують новітні матеріально-технічні бази для програмного забезпечення та передачі інформації між фізичними користувачами, підприємствами, державними установами, а разом з цим проектують новітні системи для забезпечення конфіденційності і захисту інформації. При чому, з одного боку стрімко вдосконалюються системи захисту інформації, а з іншого – не менш стрімкими темпами надходять на ринок програмних продуктів і засобів збереження і використання інформації програми для подолання інформаційного захисту, несанкціонованого (піратського) доступу до баз конфіденційних даних не лише фізичних осіб, а й державних підприємств і установ [1; 2]. Особливо гостро проблема інформаційної безпеки постала під час повномасштабного вторгнення військ Російської Федерації в Україну.

Причини, які призводять до пошкодження і спотворення інформації можуть бути, як навмисними так, і випадковими. До навмисних причин в першу чергу відносять: спотворення баз даних конфіденційної інформації, доступ до інформації сторонніми користувачами і операторами програмного забезпечення, несанкціоноване виправлення інформації з метою перебоїв в роботі державних підприємств і установ. Перебої в роботі програмного забезпечення, помилки програмістів і операторів програмного забезпечення і його дефекти можуть бути, як спричинені випадковими діями так, і навмисними. Навмисне пошкодження і спотворення програмного забезпечення спричинені цілеспрямованими шкідливими діями операторів стороннього програмного забезпечення чи втручанням зловмисників в інформаційний простір фізичних осіб і підприємств [3].

На сьогоднішній день найбільш поширеними в Україні та в інших країнах світу програмними продуктами для захисту інформації є: CD-CORS, StarForce LaserLock, SafeDisk, SecuRom, TAGES, Dallas Lock. Наведемо стислу характеристику для кожного програмного продукту.

CD-CORS застосовують для вимірювання фізичних характеристик без нанесення особливих міток на носіях даних. Через те, що ця програма заснована на методі фізичних характеристик зовнішніх носіїв інформації,

захист конфіденційної інформації з використанням програми CD-CORS вважаться найефективнішим. Цей тип захисту використовують такі комерційні продукти: English/De Agostini, Nationalencyklopedin, Agostini Atlas 99, Agostini Basereta, BMM, DK Kort, Lademanns'99.

StarForce застосовують для вимірювання фізичних характеристик без нанесення особливих міток на носій. Як і попередня система, ця система захисту інформації організована на методі вимірювання фізичних характеристик зовнішніх носіїв інформації. Цей вид захисту застосовують 1C (ігри), Нівал, Softmax Co, Q-puncture Inc, Scholastic, Hypnosys World та деякі русифіковані ігри.

Хоча LaserLock захист полягає в фізичному нанесенні мітки на носії, цей програмний продукт не здійснює захист дрібних партій (CD/R/RW). Для функціонування цього програмного продукту потрібна особлива, унікальна апаратура для захисту серії. Цю систему захисту застосовують Asghard, Fallout 2, Icewind Dale, Jagged Alliance 2, Messiah, Metro Police, Outcast, Shogo, SpecOps.

Для застосування програмного продукту SafeDisk потрібне додаткове устаткування, яке наносить фізичні мітки на носії. Цей вид захисту використаний у практично всіх іграх, випущених у масовий прокат після першого січня 2001 р. Незважаючи на те, що система захисту SecuRom використовує мітки на носіях, вона відрізняється від попередніх систем тим, що ці мітки не копіюються. Цей тип захисту використовують такі комерційні продукти: Diablo 2, SimCity 3000, Decent FreeSpace, FIFA 99, Panzer Commander, S.A.G.A: Rage of the Vikings.

Система захисту TAGES призначена для вимірювання фізичних характеристик без нанесення фізичних міток на носії. Захист інформації заснований на методі багаторазового зчитування одного і того ж сектора інформації з наступним порівнянням інформації. З недоліків вищенаведеної системи є те, що, як і система LaserLock, ця система не здійснює захист дрібних партій (CD/R/RW). Цей тип захисту використовує комерційний продукт Moto Racer.

Для захисту ресурсів персонального комп'ютера і локальної обчислювальної мережі, автоматизованого контролю і ведення протоколу дій щодо доступу до комп'ютера застосовують систему захисту Dallas Lock. Цей захист інформації ґрунтується на застосуванні персональних ідентифікаторів, які разом з паролями підвищують надійність захисту.

Незважаючи на зазначені переваги наведених новітніх програмних продуктів, які використовуються в Україні та в інших країнах світу для захисту інформації, слід врахувати, що не існує універсальних, абсолютно надійних систем захисту. Для найбільш ефективного захисту інформації потрібно спроектувати окрему систему захисту для певного виду інформації під визначені несанкціоновані дії на обговорену заздалегідь тривалість захисту.

Інформаційні джерела:

1. Дудатьєв А.В. Захист програмного забезпечення. / Дудатьєв А.В., Каплун В.А., Семеренко В.П. Вінниця: ВНТУ, 2005. Ч. 1. 140 с.

2. Levkin, A. Economic Security as a Result of Modern Biotechnology Implementation. / Levkin A., Levkina R., Petrenko A., Chaliy I. // Problems of Infocommunications. Science and

Technology (PIC S&T ‘2019): 2019 IEEE International Scientific-Practical Conference (Kyiv 8-11 October 2019). Kyiv, 2019. Pp. 139–142.

3. Левкін А. Математика як інструмент формування професійних компетентностей в ІТ-менеджменті. / Левкін А., Левкін Д., Синявіна Ю. // Новий колегіум. Харків: ХНУРЕ, 2024. № 2 (114). С. 67–71. DOI:10.34142/nc.2024.2.67

ЦИФРОВИЙ РОЗВИТОК КОНЦЕПЦІЇ SMART-БІЗНЕСУ

Мандич О.В., д-р екон. наук, проф.
Державний біотехнологічний університет

Проблеми забезпечення конкурентоспроможного розвитку українського бізнесу в сучасних умовах невизначеності та кризи внаслідок військової агресії окреслюють декілька напрямів для формування практичних платформ для сфери фінансового управління та реінжинірингу бізнес-процесів всередині підприємств. Одним з представлених напрямів є створення підґрунтя для формування методології SMART-бізнесу («розумного бізнесу»), який одночасно також базується на засадах цифрової адаптації та трансформації підприємств.

Концепція «розумного бізнесу» досліджується як українськими, так і зарубіжними вченими. На даний час існують різні думки щодо його сутності, концептуальних положень та змістовного наповнення. Так, одним з представлених форматів є розуміння «розумного бізнесу» на основі ідеї загальної функціональної допомоги для покращення бізнесу не за рахунок впровадження випадкових технологій, а через необхідність підбору правильного інструментарію для бізнес-процесів. При чому відповідний інструментарій має відповідати потребам та одночасно створювати ринкову цінність для бізнесу. За даною концепцією з метою забезпечення успіху «розумного бізнесу» та отримання гарантій його подальшого ринкового успіху, суб’єкти бізнесу мають працювати за ітераційним підходом, вивчати сильні та слабкі сторони, рівень технологічних можливостей та особливу увагу звертати на цифрову зрілість. Технологічний рівень дозволятиме знаходити правильні рішення для формування «розумного бізнесу», що також включатиме пошук нових технологічних ідей, нових технологічних можливостей, нових технологічних проєктів, які в синергії будуть створювати перед суб’єктами бізнесу реальні виклики. Залучення саме ітераційного підходу, представленого авторами, надаватиме можливості адаптації до конкретних потреб та гарантування забезпечення стійкості бізнесу, як модель у досягненні головної мети. Представлені напрями створюються для забезпечення пошуку ідеальної «відправної точки» [1, 2]. Технологічними партнерами запровадження нових адаптаційних моделей для бізнесу можуть стати програми SMART, які надають консультаційні послуги у сфері виборної підтримки, розробки, навчання та бізнес-супроводу від ERP й CRM систем. Адаптивними послугами в сфері