1.16. Безпека комп'ютерних економічних систем

Проблема захисту комп'ютерних систем є актуальною у всьому світі. Увага до цієї проблеми зумовлена стрімким розвитком комп'ютерної техніки та доступністю її широкому загалу і, як наслідок, активним використанням у багатьох сферах людської діяльності. Застосування комп'ютерних засобів для формування, обробки та зберігання інформації в економічній сфері, з одного боку, значно полегшує та прискорює роботу із інформацією, а з іншого боку, створює можливості для зловживань нею, що може мати значні негативні наслідки для організації-власника інформації.

Поняття "захист комп'ютерних економічних систем" включає три основні компоненти, які підлягають захисту: комп'ютерна система, програмні продукти, інформація користувача. На практиці загрози для інформаційно-телекомунікаційних систем можуть бути реалізовані безпосереднім впливом на інформацію, яка представляє інтерес для кінцевого користувача, або на інформаційні ресурси і телекомунікаційні служби системи. На сьогодні у світі розроблені методи і засоби як для захисту кожного із таких компонентів зокрема, так і комп'ютерних економічних систем у цілому. Найбільш актуальними є сертифіковані багатокомпонентні системи захисту, які передбачають захист інформаційних систем від різноманітних загроз. Основною метою усіх розроблених засобів захисту, включаючи апаратні, програмні та комплексні, є забезпечення інформаційної безпеки, тобто стану захищеності даних, які обробляються, зберігаються і передаються в інформаційно-телекомунікаційних системах, від незаконного ознайомлення, перетворення і знищення, а також стан захищеності інформаційно-технічних ресурсів від впливів, спрямованих на порушення їх працездатності.

Розглянемо основні загрози комп'ютерних економічних систем та шляхи їх усунення.

Комп'ютерний вірус – програма (деяка послідовність здійсненного коду або команд), що здатна створювати копії себе, і "вводити" їх у різні об'єкти системи комп'ютера. Вони зазвичай є цілком функціональними копіями і дозволяють вірусу поширюватися далі. Швидке поширення вірусу на значну кількість окремих комп'ютерів чи у мережі називається епідемією.

Віруси класифікуються за тим, де вони розміщуються у комп'ютері (файли, завантажувальні сектори), за методом інфікування (резидентний чи нерезидентний, повільний або ж швидкий), за їх здатністю до руйнування (безпечний, небезпечний, дуже небезпечний) і будь-якими спеціальними особливостями вірусного алгоритму (наприклад поліморфізм). Ознаками вірусної інфекції можуть бути: уповільнення виконання програми; збільшення розміру файла; поява нових "дивних" файлів; зменшення повної доступної пам'яті; раптова поява "дивного" відео і звукових ефектів.

Щоденно у світі з'являється, принаймні, декілька нових вірусів або нових різновидів існуючих. Однак не всі віруси, що з'явилися, можуть викликати епідемію. Користувачам комп'ютерів на допомогу створюється спеціалізоване програмне забезпечення для боротьби з комп'ютерною інфекцією – *антивіруси*.

Існує велика кількість виробників такого програмного забезпечення і пропозицій на ринку антивірусів також багато. Найчастіше на даний час використовуються антивіруси Kaspersky Anti-virus та Dr.Web.

Було досліджено чотири поширених антивірусних комплексів від різних виробників (Symantec Antivirus Corporate Edition 8.1, Kaspersky Antivirus, Ukrainian National Antivirus, Dr.Web). Метою дослідження було визначення швидкості перевірки файлів на наявність вірусної інфекції (отже, і комфортність роботи із ПК при використанні даного антивірусу) та ефективність перевірки файлів на віруси. Тестування кожного з антивірусів проводилося в чотири етапи: два тести на швидкодію і два – на якість детектування вірусів.

Ціль тестів на швидкодію полягала у вимірюванні швидкості роботи антивірусного ядра кожного із продуктів у двох режимах: настроювання за замовчуванням і максимальні настроювання роботи. Саме від швидкості роботи антивірусного ядра (швидкості перевірки одного файла) буде залежати швидкодія кожного з модулів.

Для тестування антивірусів на якість детектування вірусів було зібрано дві групи файлів: перша група – ITW (In The Wild) (ITW-вірусами називаються ті віруси, які зустрічалися в "дикому виді" (тобто в реальних користувачів, а не в лабораторних умовах або в колекціях вірусологів) віруси, друга група – збірна вірусна колекція як нових, так і старих вірусів.

1. Тести на швидкодію.

Перший тест – перевірка каталогу з настроюваннями, які встановлені в сканері за замовчуванням. Настроювання за замовчуванням для сканерів антивірусів та зведені результати тестування наведені у таблицях 1 та 2 відповідно.

Таблиця 1.

Настроювання за замовчуванням для сканерів антивірусів

Найменування антивірусу	Настроювання за замовчуванням
Dr.Web	Сканер тестує файли "за форматом", архіви, поштові бази, упаковані файли та SFX-архіви. Евристичний аналізатор налаштований на максимальний рівень перевірки
KAV	Сканер тестує всі файли й перевіряє архіви, поштові бази, вкладені об'єкти та SFX-архіви
UNA	Сканер тестує "розширений набір" файлів і перевіряє архіви. Евристичний аналізатор відключений
SAV	Сканер тестує всі файли й перевіряє архіви із вкладенням до 3-х

Таблиця 2.

Зведені результати тестування на швидкодію при настроюваннях за замовчуванням

Найменування антивірусу	Швидкість тестування (файлів у секунду)	Усього перевірено файлів	Витрачений час, с
Dr.Web	17,39	6607	380
KAV	17,26	11962	693
UNA	20,61	5792	281
SAV	8,44	7651	907

Другий тест – перевірка каталогу з максимальними настроюваннями, але при відключеній перевірці архівів. Для тестування використовувалась та ж система, що й для попереднього тесту. Для всіх програм були встановлені наступні настроювання: перевіряються всі файли, тестування архівів і поштових баз відключене, евристичний аналізатор включений на максимум. Результати тестування наведені у таблиці 3.

2. Перевірка на детектування ITW вірусів/

Для проведення тесту було відібрано 593 віруси (за основу брався список, наведений на сайті WildList.com і використовуваний при тестуванні англійським журналом Virus Bulletin. З нього були видалені віруси, які не зустрічалися на території України за останні місяці й додані ті віруси чи трояни, які не фігурують в VB-списку, однак зафіксовано їх кількаразову появу в кінцевих користувачів на території СНД), які були зафіксовані в дикому виді протягом останніх двох місяців.

Таблиця 3

Зведені результати тестування антивірусів на швидкодію при максимальних настроюваннях

Найменування антивірусу	Швидкість тестування (файлів у секунду)	Усього перевірено файлів	Витрачений час, с
Dr.Web	12,00	3168	264
KAV	9,70	3201	330
UNA	5,97	3126	524
SAV	5,26	3128	595

При проведенні даного тесту основним завданням антивірусів було детектування максимальної кількості вірусів, у зв'язку із цим всі сканери були настроєні на максимальний рівень перевірки.

Тест здійснювався в такий спосіб:

1. На "чисту" (настроєну систему, у якій відсутні антивірусні продукти) установлюється антивірусний продукт для тестування, антивірусні бази продукту доводять до актуального стану.

2. Запускається сканер з інтерфейсом GUI (якщо є кілька варіантів інтерфейсу, запускається професійний варіант) і його настроювання вставлюються в стан максимальної якості детектування (на максимум включаються всі модулі евристичного сканування, підключаються всі бази).

3. Як об'єкт тестування вибирається папка, що містить колекцію вірусів у вигляді набору інфікованих файлів, зібраних для тестування продуктів.

4. Запускається сканування в режимі створення звіту із записом в log-файл (без виконання дій над інфікованими файлами).

5. По закінченні виконання тестування отриманий звіт про тестування зберігається і оцінюються остаточні результати роботи: кількість перевірених об'єктів, кількість виявлених інфікованих файлів, кількість виявлених "підозрілих" файлів.

6. Система відновлюється у стан до виконання п. 1 і починається тестування наступного антивірусного продукту.

Результати тестування наведені у таблиці 4.

Таблиця 4

Зведені результати тестування на детектування ITW вірусів

Антивірус	Відсоток виявлення	Перевірено	Кількість тіл вірусів	Кількість підозрілих файлів
Dr.Web	97,65	593	582	1
KAV	100,00	593	593	–
UNA	100,00	593	593	–
SAV	94,60	593	561	–

3. Тест на розгорнутій колекції вірусів

Тест був проведений на тій же системі, що й ITW-тест. Для тестування використовувався розширений набір вірусів. Розмір колекції становив близько 2,5 Gb і нараховував більше 30 тисяч інфікованих файлів. Головним завданням антивірусів було детектування максимальної кількості інфікованих файлів. Результати тестування наведені у таблиці 5.

Таблиця 5

Зведені результати тестування на розгорнутій колекції вірусів

Назва продукту	Виявлено тіл вірусів	Виявлено модифікацій вірусів	Виявлено підозрілих файлів	Усього файлів перевірено	Витрачений час, хв, с
Dr.Web	27930	472	720	31372	30:05
KAV	30814	7	18	31262	30:12
UNA	30976	–	62	31206	25:14
SAV	Тест не пройдений			29966	> 934

Одним із сучасних методів *захисту матеріальних носіїв інформації* є нанесення на них голографічних знаків. *Голограма* визнана ефективним інструментом захисту від підробок, оскільки задовольняє всім вимогам безпеки інформації. Голограма може поставлятися замовнику і наноситися на носій інформації ним безпосередньо в момент випуску документа або впровадження в обіг у відриві від поліграфічного процесу. Тому необхідно правильно будувати систему контролю, при якій оптимально сполучаються централізація і відповідальність кожного рівня виконання за розкрадання й несанкціоноване тиражування захисних елементів. Необхідне створення єдиного реєстру голографічних захисних елементів з описом ознак достовірності.

Застосування голографічних знаків дає можливість захищати матеріальні носії інформації шляхом засвідчення їх достовірності. До таких носіїв, у першу чергу, належать паперові документи та компакт-диски. Методи захисту гнучких дисків базуються на двох принципах: або перешкодити копіюванню програми на інший диск чи знищити її, або перешкодити перегляду чи операції реасемблювання, що дозволяє представити програму у формі, доступній для сприйняття. Захист інформації, що зберігається на жорстких дисках, включає в себе обмеження доступу та унеможливлення несанкціонованого доступу до останніх. Існує кілька шляхів вирішення цього питання, що вимагають застосування різних організаційних і технічних заходів.

Найкращий і найпростіший спосіб – це не залишати диски із критичною інформацією без контролю. Для реалізації такого способу існують спеціальні фрейми швидкої установки й зняття жорстких дисків. Такі фрейми можуть установлюватися в корпус комп'ютера і підключатися до комп'ютера через інтерфейс USB або FireWare. Жорсткий диск у знімному фреймі зберігається в приміщенні, що охороняється (у секретному відділі) і видається користувачу під розписку тільки на час роботи.

Другий спосіб забезпечення неможливості несанкціонованого доступу до інформації – це її шифрування. Шифрування може здійснюватися апаратно, засобами BIOS комп'ютера, засобами операційної системи або спеціалізованими програмами (PGP, WinRar 2.6). З погляду надійності обмеження несанкціонованого доступу, принципової різниці у виборі способу шифрування немає. Основним питанням постає забезпечення неможливості несанкціонованого доступу до ключів шифрування. Частково проблеми, пов'язані з обмеженням доступу до ключів шифрування вирішуються шляхом зберігання ключів на зовнішніх носіях. Зокрема, можуть застосовуватися неспеціалізовані пристрої (Flash-карти) або спеціально розроблені носії: TouchMemory, SmartCard, ключі HASP, e-Token.

Схоронність носіїв ключової інформації може бути забезпечена організаційними заходами.

Шифрування дозволяє надійно вирішити завдання обмеження доступу до інформації (при правильній організації генерації, зберігання й розподілу ключів).

Найбільш поширеними програмами захисту інформації серед користувачів є програмні комплекси Wipeinfo, програма з пакета Norton Utilities Diskreet.exe, програма присвоєння паролів Password.exe з операційної системи Novell Dos. Програма Diskreet.exe з пакета Norton Utilities, дає можливість створити додатковий логічний драйвер з вільного дискового простору. При цьому є можливість використовувати шифрування даних та підключення цих драйверів у міру необхідності.

Для захисту окремих каталогів та файлів також можна використовувати зміну їх атрибутів або можливості доступу на рівні профілів користувачів.

Захист інформації, що міститься на накопичувачах на жорстких магнітних дисках (НЖМД), протягом її життєвого циклу та періоду експлуатації НЖМД здійснюється різноманітними технічними і нетехнічними (програмними, апаратними, фізичними, адміністративними) методами. Однак на даний час значної уваги потребує також питання забезпечення надійного знищення корпоративної інформації наприкінці життєвого циклу НЖМД, оскільки одержання інформації зловмисником може призвести до значних збитків для організації. Процес знищення інформації повинен ґрунтуватися на ряді узгоджених методик, що забезпечують в остаточному підсумку високу ймовірність знищення інформації.

Процедура забезпечення захисту інформації, збереженої на НЖМД, повинна включати наступні дії:

1. Фізичний захист інформації, що включає в себе інвентаризацію та обмеження доступу.
2. Систематичний контроль над процесом заміни, передачі й знищення інформації.
3. Використання стандартизованих додатків і методик зі знищення інформації.
4. Систематична перевірка процесів знищення інформації.
5. Періодичний контроль надійності знищення інформації з довільно обраних накопичувачів.
6. Вибір методик і способів для знищення інформації на несправних НЖМД, шляхом аналізу категорійності збереженої на них інформації.
7. Забезпечення процедури збору і знищення накопичувачів.
8. Ведення звітності за кожним знищеним НЖМД.

Способи знищення інформації на НЖМД діляться на три групи:

1. Програмні, в основу яких покладене знищення інформації, записаної на магнітному носії, за допомогою штатних засобів запису інформації на магнітних носіях.

2. Механічні, пов'язані з механічним пошкодженням основи, на яку нанесений магнітний шар – фізичний носій інформації.

3. Фізичні, пов'язані з фізичними принципами цифрового запису на магнітний носій, і засновані на перебудові структури магнітного матеріалу робочих поверхонь носія.

Є два різних типи *захисту доступу до загальних ресурсів*: захист на рівні ресурсів та захист на рівні користувачів.

Схема забезпечення захисту на рівні ресурсів (використовується в Windows for Workgroup) передбачає встановлення пароля для кожного загального ресурсу. Будь-який користувач, який бажає отримати доступ до загального ресурсу, повинен вказати цей пароль.

Захист на рівні користувачів – схема, яка надає доступ до загального ресурсу визначеним користувачам, запит на використання ресурсу передається на Windows NT сервер, який порівнює ім'я користувача та пароль і визначає можливість доступу. Якщо пароль є коректним, користувач отримує право на використання ресурсу. Обмеження прав доступу може встановлюватись як для апаратних, так і для програмних засобів.

Системи безпеки бувають двох видів:

1. Доменна система безпеки – складна система прав мережного доступу, яка дозволяє адміністраторам використовувати жорсткий поділ прав доступу до інформації та ресурсів мережі. Контролери доменів відповідають за перевірку запитів користувача на реєстрацію в мережі. Інформація про права доступу зберігається в спеціальній базі прав доступу – диспетчері системи безпеки, яка періодично оновлюється.

2. Файлова система безпеки. Такі системи безпеки засновані на можливостях файлових систем, наприклад NTFS. Система дає змогу адміністраторам використовувати багато різних рівнів розмежування доступу для користувачів та їх груп, починаючи з апаратних та програмних комплексів і завершуючи окремими каталогами та файлами.

Реєстрація – єдина функція, що не захищає мережу від загроз, а дозволяє виявити їх появу. Реєстрації підлягають наступні події: вхід і вихід користувача з мережі, запуск мережних додатків, звертання до файл-серверів і логічних дисків (папок) із критичними даними, факти відмови в доступі до певних ресурсів і т.д. Реалізується служба реєстрації і спостереження в реальному режимі часу за допомогою "Аудитора подій" і "Системного монітора" із складу операційної системи Windows NT Server 4.0.

Алгоритми, які усувають надмірність запису даних, називаються *алгоритмами стиску даних*, або *алгоритмами архівації*. У наш час існує багато програм для стиску даних, заснованих на декількох основних алгоритмах:

1) без втрат, при використанні яких дані відновлюються без найменших змін;

2) із втратами, які видаляють із потоку даних інформацію, що незначно впливає на суть даних, або взагалі несприйману людиною (такі алгоритми зараз розроблені тільки для аудіо- і відеозображень). У криптосистемах використовується тільки перша група алгоритмів.

Існує два основних методи стискування без втрат:

– алгоритм Хаффмана (англ. – Huffman), орієнтований на стискування послідовностей байтів, не зв'язаних між собою;

– алгоритм Лемпеля-Зіва (англ. – Lempel, Ziv), орієнтований на стискування будь-яких видів текстів, тобто використання факту кількаразового повторення "слів" – послідовностей байт.

Практично всі популярні програми архівації без втрат (ARJ, RAR, ZIP і т.п.) використовують поєднання цих двох методів – алгоритм LZH.

Найпростіші архіватори працюють за схемою "із файла в файл". Більш складні архіватори дозволяють працювати з декількома файлами одночасно. В одному структурованому файлі програма-архіватор зберігає декілька стиснутих образів файлів, а також атрибути файла (ім'я, розмір, контрольна сума). Архів побудований так, що можна мати прямий доступ до будь-якого файла. За такими схемами працюють архіватори ARJ, PKZIP/PKUNZIP, LHA, RAR, AIN. Інша група архіваторів призначена для стискування виконуваних файлів: PKLITE, LZEXE, DIET, AINEXE. Такі архіватори стискують програми, дописуючи в них модуль розпакування, що при запуску розпаковує вихідну програму. Виконувати архівацію файлів та папок можна за допомогою програмних оболонок архіваторів або через їх вбудовувані в операційну систему компоненти. Більшість архіваторів мають можливість одночасно зі стискуванням виконувати шифрування інформації. Разом зі стандартними програмами архівування використовуються так звані ущільнювачі дисків: Double Space, Driver Space, Stacker тощо. Вони працюють у реальному режимі і дають можливість архівувати і розархівовувати програми в міру звертання до них. При цьому інформація зберігається на диску в стиснутому вигляді.

Криптосистема складається із одного або декількох алгоритмів шифрування (математичних формул), ключів, які використовуються алгоритмами шифрування, підсистеми управління ключами, незашифрованого і зашифрованого текстів. До тексту, який потрібно зашифрувати, застосовують алгоритм шифрування і ключ для отримання зашифрованого тексту. Потім зашифрований текст передається до місця призначення, де той самий алгоритм використовується для його розшифрування, щоб одержати розшифрований текст.

В основі криптографічних алгоритмів лежать математичні перетворення, що дозволяють домагатися високої практичної стійкості більшості асиметричних алгоритмів шифрування. Було доведено, що в криптографії існують тільки два основних типи перетворень – *заміни* і *перестановки*, всі інші є лише комбінацією цих двох типів. Таким чином,

є криптографічні алгоритми, побудовані на основі заміни, перестановки і об'єднання цих двох перетворень.

Під *стеганографією* розуміють метод організації зв'язку, який по суті приховує саму наявність зв'язку. Стеганографія не замінює, а доповнює криптографію. Стеганографічне приховування повідомлення значно зменшує ймовірність виявлення факту передачі повідомлення, а якщо це повідомлення ще й зашифроване, то воно має додатковий рівень захисту.

Комп'ютерна стеганографічна система (*стегосистема*) являє собою сукупність засобів і методів, які використовуються для формування прихованого каналу передачі інформації. При передачі повідомлення використовується певний носій (контейнер), призначений для приховування таємних повідомлень. Стеганографічне повідомлення супроводжується передачею стегоключа. За аналогією з криптографією, за типом ключа стегосистеми поділяють на два типи: з секретним і відкритим ключем.

У стегосистемі з секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий захищеним каналом.

У стегосистемі з відкритим ключем для вкладання і добування повідомлення використовуються різні ключі, які відрізняються тим, що з допомогою обчислень неможливо вивести один ключ з іншого. Тому один ключ (відкритий) може передаватись незахищеним каналом.

Для того, щоб прихована інформація залишилась невиявленою, не повинно бути помітно, що над зображенням були проведені певні операції. Найбільш популярний спосіб, що дозволяє реалізувати таке приховування, – це LSB-алгоритм (Least Significant Bit). При цьому приховуваний файл біт за бітом включається в окремі пікселі, в останню позицію двійкового числа. LSB-алгоритм здійснює найменший вплив на значення двійкового числа.

Отже, можна виділити три пов'язані між собою напрями застосування стенографії: приховування повідомлень, цифрові водяні знаки і заголовки.

Приховування великих повідомлень має значні вимоги до контейнера, адже його розмір має в декілька разів перевищувати розмір приховуваних даних. Цифрові водяні знаки використовуються для захисту авторських прав на цифрові зображення та інші оцифровані витвори мистецтва. Заголовки використовуються для маркування зображень у великих електронних сховищах, цифрових зображень, аудіо- та відеофайлів.

Наявність *цифрового підпису* в повідомленні електронної пошти надає одержувачу досить високий рівень впевненості у істинності відправника. Цифровий підпис також використовується для шифрування

і дешифрування повідомлень. Загальна схема використання цифрового підпису полягає в наступному:

PGP (Pretty Good Privacy) – це криптографічна (шифрувальна) програма з високим ступенем надійності, що дозволяє користувачам обмінюватися інформацією в електронному вигляді в режимі повної конфіденційності.

Головна перевага цієї програми полягає в тому, що для обміну зашифрованими повідомленнями користувачам немає необхідності передавати один одному таємні ключі, оскільки програма побудована за принципом публічної криптографії або обміну відкритими (публічними) ключами, де користувачі можуть відкрито надсилати один одному свої публічні ключі за допомогою мережі Інтернет.

Отже, у зв'язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз їх захищеності проблема безпеки комп'ютерних економічних систем потребує постійної уваги. В сучасних умовах захист комп'ютерних економічних систем може бути забезпечений тільки комплексною системою захисту інформації, яка повинна бути безперервною, плановою, цілеспрямованою, конкретною, активною, надійною.

Список літератури:

1. Богуш В.М. Інформаційна безпека держави. – К.: «МК-Прес», 2009. – 432с.
2. Довгань О.Д. Методологія захисту інформації. – К. : НаСБУ, 2012. – 227с.
3. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. – К. : Київ. нац. торг. екон. ун-т, 2001. – 309 с.
4. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. [Електронний ресурс]. – Режим доступу: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php
5. Ткачук Т. Формування системи інформаційної безпеки бізнесу // Бізнес і безпека, 2009. – №4. – С.19-23.

1.17. Еволюція підходів до аналізу та моделювання поведінки рахунку поточних операцій платіжного балансу країн

Поточний рахунок є відображенням ефективності макроекономічної політики та джерелом інформації про поведінку економічних агентів в країні [12]. З одного боку, він відображає сукупність операцій резидентів з нерезидентами на ринку товарів та послуг, а з іншого – міжчасові рішення резидентів та нерезидентів в контексті інвестування та заощадження. У відкритих економіках зміни сальдо поточного рахунку тісно пов'язані з діями та очікуваннями всіх учасників ринку. Саме тому поточний рахунок вважають