УДК 004.380

Фенко О.Г., Лисенко Д.І.

ПОЛІТИКА БЕЗПЕКИ: ЗАДАЧІ І РІШЕННЯ

Полтавський національний технічний університет імені Юрія Кондратюка,
Полтава, пр-т. Першотравневий 24, 36011

Fenko O.G., Lysenko D.I.

POLICY OF SAFETY: TASKS AND DECISIONS

Poltava National Technical University named after Yuri Kondratyuk,
Poltava, Ave. Pershotravnevuy 24, 36011

Анотація. У роботі розглядається проблемне питання політики інформаційної безпеки. Ріст кібезлочинності - двигун до розвитку нових напрямків і технологій у сфері захисту і безпеки інформації. Це напрямок захисту програмних продуктів, проактивний захист від шкідливого ПЗ (задача захисту виявити уразливі місця раніш хакера), захист текстів інтернет-сторінок, захист баз даних, контроль за витоком інформації й отут не можна обійтися без аналізу фінансових втрат, тому, коли підприємство розробляє політики безпеки - це завжди індивідуально, але класичні теорії і сучасні технології єдині для усіх. При розробці будь-якої автоматизованої системи паралельно йде розробка політики безпеки.

Ключові слова: захист програмних продуктів, захист баз даних, політика безпеки, кіберзлочин

Abstract. The problem question of policy of informative safety is in-process examined. A height of cybercrime is an engine to development of new directions and technologies in the field of defence and safety of information. It is direction of defence of programmatic foods, proactive protecting from harmful programs (task of defence to find out vulnerable places before hacker), defence of texts of internetpages, defence of bases given, control after the source of information and it is

here impossible to do without the analysis of financial losses, volume, when an enterprise develops politicians of safety - it always individually, but classic theories and modern technologies are only for all. At development of any CAS development of policy of safety goes in parallel.

Key words: defence of programmatic foods, defence of bases given, politician of safety, cybercrime

Вступ.

Інформаційні процеси у світі висувають на перший план, поруч із задачами ефективної обробки і передача інформації, забезпечення безпеки інформації, особливо в системах телекомунікацій, що обслуговують банківські, торгівельні установи і службу держбезпеки. Ступінь небезпеки електронних злочинів можна визначити по тим витратам на засоби захисту, що вважаються припустимими і доцільними. Останнім часом також різко зросла кількість випадків крадіжки програм у комп'ютерних мережах, що набуло характер епідемії: на кожну законну копію більш – менш популярної програми, існує кілька копій, отриманих незаконним шляхом. Оскільки основний інформаційний обмін заснований на інформаційних технологіях, важливою умовою безпеки стає безпека в комп'ютерних мережах.

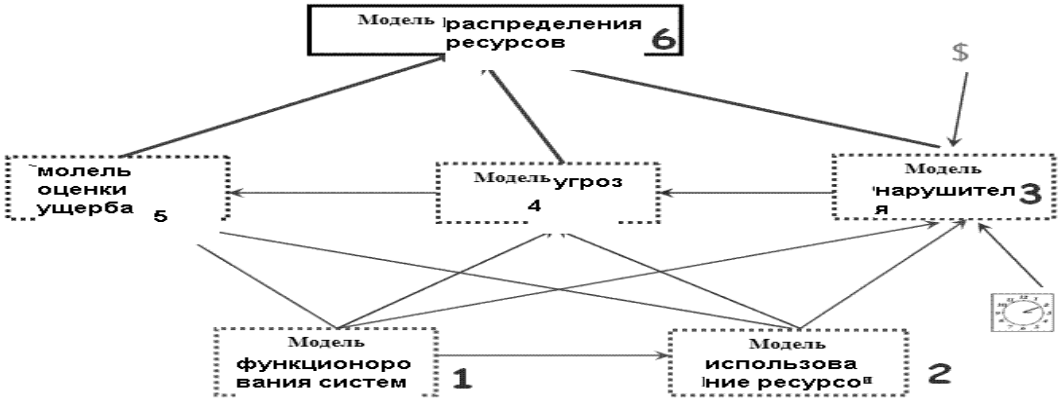
Огляд літератури.

Сьогодні фахівці із самих різних областей знань, так чи інакше, змушені займатися питаннями забезпечення інформаційної безпеки. Це обумовлено тим, що в найближчі років сто нам доведеться жити в суспільстві (середовищу) інформаційних технологій, куди перекочують усі соціальні проблеми людства, у тому числі і питання безпеки. У своїй роботі експертом Домаревим В.У викладені причини порушення безпеки комп'ютерних систем, приведений опис математичних моделей систем захисту інформації, а також розглянуті методи і засоби впровадження механізмів захисту в існуючі інформаційні системи з можливістю гнучкого керування безпекою в залежності від висунутих вимог, припустимого ризику й оптимальної витрати ресурсів [1],[2]. Г.Е. Шепітько у своїй роботі дав аналіз захисту інформації, нейтралізації порушника,

можливості комплексного підходу до політики безпеки [3],[4]. З метою підвищення стійкості результатів категорування інформації, що містить комерційну таємницю автором пропонується збільшити кількість категорій і ознак, при цьому формалізувати алгоритм класифікації на базі теорії нечітких безлічей [5].

Основний текст.

Аналіз захищеності операційної системи (ОС) з погляду системності. Поняття системності полягає не просто в створенні відповідних механізмів захисту, а являє собою регулярний процес, здійснюваний на всіх етапах життєвого циклу ОС. На моделі (мал.1) представлена послідовність взаємодії функціонування системи і модель дій порушника.



Мал.1 „Модель ресурси системи – порушник”

ОС повинна сприяти реалізації заходів безпеки або прямо підтримувати їх. Приклади подібних рішень у рамках апаратури й операційної системи - поділ команд по рівнях привілейованості, захист різних процесів від взаємного впливу за рахунок виділення кожному свого віртуального простору, особливий захист ядра ОС, контроль за повторним використанням об'єкта. Основною проблемою при захисті й оцінці уразливих місць в операційних системах є контроль доступу, що реалізується на рівні користувачів. У залежності від задач, які потрібно вирішувати за допомогою обчислювальної системи, обирається тип контролю доступу, що буде введений в інформаційну систему. Помилка в питанні розмежування прав між користувачами може привести до витоку важливої інформації, її спотворення або повної втрати. Списки

контролю доступу є одним з можливих методів захисту інформаційних ресурсів в операційній системі. Оскільки число користувачів різних автономних систем невпинно зростає, актуальним стає питання розмежування їхніх повноважень в інформаційній системі. Існує 2 типи списків контролю доступу. Перший працює на рівні користувачів і представляє механізм захисту ресурсів, таких як файли і папки. Другий тип контролю доступу – це системний список керування доступом і механізм контролю над повідомленнями аудиторові, що пов`язаний з інформаційним ресурсом, тобто кількість успішних і невдалих спроб доступу. Робота списків контролю доступу базується на створенні записів контролю доступу, у яких поєднується ідентифікатор безпеки користувача з маскою доступу. Запис контролю доступу може як дозволяти так і забороняти право на використання визначеного ресурсу. Кожен запис зберігається в базі даних, що знаходиться в метафайлі $Secure файлової системи NTFS (Windows NT та подальші). Для розробки програми, за допомогою якої буде реалізовуватися призначення прав доступу до ресурсів операційної системи необхідно використовувати API-функції і бібліотеку класів .NET Framework, що містить простір імен System.Security. AccessControl. Звичайно кожен користувач у системі має унікальний ідентифікатор. Ідентифікація полягає в повідомленні користувачем свого ідентифікатора. Для того щоб встановити, що користувач саме той, за кого себе видає, тобто що саме йому належить введений ідентифікатор, в інформаційних системах передбачена процедура аутентифікації (authentication, упізнання, у перекладі з латинської - встановлення дійсності), задача якої - запобігання доступу до системи небажаних осіб. Звичайно аутентифікація базується на одній або декількох основах: 1)те, чим користувач володіє (ключ або магнітна карта), 2)те, що користувач знає (пароль), 3)атрибути користувача. Для збереження секретного списку паролів на диску більшість ОС використовують криптографію. Система використовує однобічну функцію, що надзвичайно важко (розробники сподіваються, що неможливо) інвертувати, але просто обчислити. Зберігаються тільки кодовані паролі. У процесі аутентифікації

пред`явлений користувачем пароль кодується і порівнюється з тим, що на диску тому, файл паролів немає необхідності тримати в секреті. Основні напрямки використання криптографічних алгоритмів - передача конфіденційної інформації з каналів зв'язку (наприклад, електронна пошта), перевірка автентичності переданих повідомлень, збереження інформації (документів, баз даних; у криптографії й інформаційній безпеці цілісність даних (у широкому сенсі) — це збереження даних у тому вигляді, у якому вони були створені. Приклади порушень цілісності даних: спроба зловмисника змінити номер акаунта в банківської транзакції або спроба підробки документа; випадкова зміна інформації при передачі або при несправній роботі жорсткого диску; перекручування фактів засобами масової інформації з метою маніпуляції суспільною думкою. Цілісність інформації (також цілісність даних) — термін в інформатиці (криптографії, теорії телекомунікацій, теорії інформаційної безпеки), який визначає, що дані не були змінені при виконанні будь якої операції над ними, як то передача, збереження або відображення. У телекомунікації цілісність даних часто перевіряють, використовуючи хеш-сумму повідомлення, обчислену алгоритмом MAC (англ. message authentication code). Тепер зручно використовувати терміни: computer contaminant (computer — комп'ютер і contaminant — забруднювач) для позначення шкідливого програмного забезпечення (ПЗ), що використовується в законодавстві деяких штатів США, наприклад Каліфорнії і Західної Вірджинії; crimeware (crime - злочинність і software - програмне забезпечення) - клас шкідливих програм, спеціально створений для автоматизації фінансових злочинів. Це не синонім терміна malware (значення терміна malware ширше), і не всі програми, що відносяться до crimeware, є шкідливими, оскільки поняття злочину суб'єктивно і залежить від законодавства конкретної країни, а шкода, нанесена власникові і/або користувачеві комп'ютера - об'єктивна. У будь-якому випадку це робота з програмними продуктами, отже треба зробити їхню роботу безпечної, тому проаналізуємо керування безпекою програм (табл.1).

Таблиця 1

Залежність керування безпекою програм від виду факторів небезпеки

Фактор	Керування		
	Тестування	Контроль	Контрзаходи
Дефекти	Локалізація	Інспекція ПО	Безпечне програмування
Вразливості	Ідентифікація, сканування	Поточний контроль цілісності	Виправлення
Загрози	Формування моделі загроз	Моніторинг	Блокування, фільтрація
Ризик	Оцінка ризику	Спостереження за джерелом загроз	Аналіз ризику

В розмежуванні доступу до об'єктів ОС розрізняють дискреційний (виборчий) спосіб керування доступом і повноважний (мандатний). При дискреційному доступі визначені операції над визначеним ресурсом забороняються або дозволяються суб'єктам або групам суб'єктів. З концептуальної точки зору поточний стан прав доступу при дискреційному керуванні описується матрицею, у рядках якої перераховані суб'єкти, а в стовпцях - об'єкти забезпечення захищеності інформації, розміщеної в комп'ютерному середовищі. Аналізуючи вірусну активність за 2013-2014 рік на основі звернень у службу техпідтримки було виявлено: використання соціальної інженерії, використання вразливостей, поява спеціалізованих загроз. Аналізуючи досвід виявлення вразливості робимо висновок, що основний напрямок роботи, це перевірка первинного коду ПЗ з наступною сертифікацією. Використовуючи багаторівневу систему захисту, важливо забезпечити баланс надійності всіх рівнів. Якщо в мережі всі повідомлення шифруються, але ключі легкодоступні, то ефект від шифрування нульовий. А якщо в мережі мається пристрій, що аналізує весь вхідний трафік і відкидає кадри з визначеною,

заздалегідь заданою зворотною адресою, то при відмові він повинний повністю блокувати вхід у мережу. Принцип єдиного контрольного - пропускного пункту – весь вхідний у внутрішню мережу і вихідний у зовнішню мережу трафік повинний проходити через єдиний вузол мережі, наприклад міжмережевий екран. У протилежному випадку, коли в мережі мається безліч користувальних станцій, що мають незалежний вхід у зовнішню мережу, дуже важко скоординувати правила, що обмежують права користувачів внутрішньої мережі при доступі до серверів зовнішньої мережі. Жодна система безпеки не гарантує захисту даних на рівні 100%, оскільки є результатом компромісу між можливими ризиками і витратами. Визначаючи політики безпеки, адміністратор повинний зважити величину збитку, що може понести підприємство в результаті порушення захисту даних, і співвіднести її з величиною витрат, необхідних для забезпечення безпеки цих даних. З'ясувалося, що багато користувачів дотепер не знають основи мережної безпеки. Через це соціальна інженерія (керування діями людини без використання технічних засобів) стала найбільш популярною тенденцією 2013 року. Хакери активно використовували уразливості платформи Java тому, що вона є одним з найбільш слабких елементів у захисті операційних систем, на яких встановлена. У світлі концепції кіберзахисту в різних країнах актуальна проблема порушення роботи стратегічних об`єктів, проведення мережного шпигунства, використання транзитних IP-адрес і помилкових проксі-серверів, не менш важлива фільтрація при вході у мережу, розумне використання брандмауерів, з огляду на наявність “чорного шухляди“. Банківська і фінансова сфера не можлива без мережних баз даних, от і проблема транцзакцій і SQL-ін`єкцій. В теорії баз даних цілісність даних, це коректність даних і їхня несуперечність. Звичайно вона також включає цілісність зв'язків, що унеможливлює помилки зв'язків між первинним та вторинним ключем.

Заключення та висновки.

Проведений аналіз потенційних погроз і запропоновані системи захисту від них розширюють загальний зміст теорії захисту. Безпечна інформаційна

система – це система, що, по-перше, захищає дані від несанкціонованого доступу, по-друге, завжди готова надати їх своїм користувачам і по-третє, надійно зберігає інформацію та гарантує незмінність даних.

Література:

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ТИД "ДС", 2002. 688 с.

2. Домарев В.В. Безопасность информационных технологий. Системный подход. Киев: ООО ТИД «Диасофт», 2004. 92 с.

3. Шепитько Г.Е. Социальная эффективность нейтрализации высококвалифицированных нарушителей информационной безопасности. М.: Академия ГПС МЧС России, 2011. 41 с.

4. Дэвид Феррайоло, Ричард Кун Role-Based Access Controls

5. Шепитько Г.Е. Категорирование объектов информатизации

Стаття відправлена: 18.05.2015р.