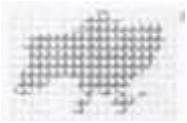
Міністерство освіти і науки України

Український науковий центр розвитку інформаційних технологій
(УкрНЦ РІТ)



**Шевченко В.Л., Нестеренко О.В.,
Нетесін І.Є., Шевченко А.В.**

Прогностичне моделювання комп'ютерних вірусних епідемій

Монографія

УкрНЦ РІТ
Київ
2019

УДК 004.49
П-163

Рекомендовано до видання Вченою радою Національної академії управління (Протокол № 3 від 29 березня 2019 року)

Прогностичне моделювання комп'ютерних вірусних епідемій / [Шевченко В.Л., Нестеренко О.В., Нетесін І.Є., Шевченко А.В.]; за ред. В.Б. Поліщука. – Київ: УкрНЦ РІТ, 2019. – 152 с.

Рецензенти:
1. *Гайдур Галина Іванівна*, доктор технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій.
2. *Зінченко Андрій Олександрович*, доктор технічних наук, доцент, начальник кафедри зв'язку та АСУ Національного університету оборони України імені Івана Черняховського.

Монографію присвячено методам створення прогноз-моделей розвитку комп'ютерних вірусних епідемій. Проаналізовані основні види інцидентів інформаційної безпеки. Надані основні класифікації щодо комп'ютерних атак та способів захисту. Встановлений зв'язок між параметрами математичних моделей та прикладними заходами протидії зараженню інформаційних систем.

Монографія адресована фахівцям з питань захисту інформації в мережевих інформаційних системах, викладачам вищих навчальних закладів, студентам та аспірантам.

Монографію написано колективом авторів у складі: В.Л. Шевченко (розділ 3); О.В. Нестеренко (розділи 1, 2); І.Є. Нетесін (розділ 2); А.В. Шевченко (розділ 3).

ISBN 978-966-97923-0-3

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС - автоматизована система
ІБ - інформаційна безпека
ІТ - інформаційні технології
ІС - інформаційна система
НСД - несанкціонований доступ
ОС - операційна система
ОУ - орган управління
ПЗ - програмне забезпечення
ПК - персональний комп'ютер

Адекватний захист – оптимальний випадок, коли реальні результати з достатньою точністю збігаються з суб'єктивною оцінкою параметрів загрози.

Антивірус – 1) програма, що лише виявляє або виявляє і видаляє віруси. Якщо вірус видалити не вдається, заражена програма знищується;

2) програма, призначена для захисту від вірусів, виявлення заражених програмних модулів і системних ділянок, а також відновлення початкового стану заражених об'єктів.

Аналіз загроз – один із найважливіших розділів аналітичної роботи, що визначає відповіді на питання від чого або від кого варто захищати об'єкти захисту.

Апаратний захист (Hardware security) – використання апаратних засобів, наприклад, регистрів меж або замків і ключів для захисту даних в комп'ютері.

Аплети – невеликі застосування, написані різними мовами програмування, які автоматично завантажуються і виконуються WWW-браузерами, що підтримують аплети.

Атака (Attack) – порушення безпеки інформаційної системи, що дозволяє порушнику управляти середовищем системи; або зловмисна дія, основна мета якої одержати НСД до інформації, спроба реалізації будь-якого виду загрози.

Атестація засобів захисту (Endorsment) – засвідчення ступеню відповідності до вимог даного класу засобів захисту.

Аудит (Audit) – реєстрація подій, що впливають на безпеку системи, з метою надання інформації для подальшого відновлення безпеки системи.

Багаторівнева атака – концепція (модель) доступу суб'єктів з різними правами до об'єктів різних рівнів секретності.

Безпека (Safety, security) – стан захищеності життєво важливих інтересів особи, суспільства й держави в різних сферах життєдіяльності, а також довкілля від внутрішніх і зовнішніх загроз.

Безпека інформаційної системи (Information system security) – 1) властивість системи протистояти спробам несанкціонованого доступу до оброблюваної інформації, що зберігається;

2) сукупність заходів з управління і контролю, які захищають ІС від відмови в обслуговуванні і несанкціонованого (умисного або випадкового) розкриття, модифікації або руйнування ІС і даних.

Безпека даних (Data security) – захист даних від несанкціонованої (випадкової або умисної) модифікації, руйнування або розкриття.

Безпека інформації (Information security) – стан інформації, при якому виключаються випадкові або умисні несанкціоновані дії на інформацію або несанкціоноване її отримання.

Брандмауер (Firewall) – метод захисту мережі від зовнішніх загроз, джерелами яких є інші мережі та системи, за допомогою централізації доступу до мережі й контролю над ним апаратно-програмними засобами.

Віддалена атака – інформаційний руйнуючий вплив на ІС, що програмно здійснюється каналами зв'язку.

Вірус комп'ютерний (Virus) – спеціально написана, як правило, незначна за розмірами програма, що виконує різні небажані (частіше шкідливі) дії на комп'ютері і може "приписувати" себе до інших програм, тим самим "заражаючи" їх. Поняття «комп'ютерний вірус» часто застосовується відносно всіх типів шкідливих програм.

Власник інформації (Owner) – суб'єкт інформаційних стосунків, що має право володіння, розпорядження і користування інформаційним ресурсом згідно договору з володарем інформації.

Доступ (Access) – надання даних системі обробки даних, або отримання їх з неї шляхом виконання операцій пошуку, читання і (чи) запису даних.

Доступ до інформації – процес ознайомлення з інформацією, її документування, модифікація або знищення, що здійснюється з використанням штатних програмно-технічних засобів.

Доступність (Availability, accessibitity) - властивість ресурсу ІС, що полягає в можливості його використання на вимогу користувача, який має відповідні повноваження.

Загроза – можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент в межах даної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків, погіршити стан довкілля тощо.

Захист (Protection, security, lock out) – засіб для обмеження доступу чи використання усієї або частини інформаційної системи; юридичні, організаційні і технічні, у тому числі програмні заходи запобігання несанкціонованого доступу до апаратури, програм і даних.

Захист інформації – комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Зазвичай мається на увазі підтримка цілісності, доступності і, якщо потрібно, конфіденційності інформації і ресурсів, що використовуються для введення, зберігання, обробки і передачі даних.

Захищеність системи (System protections) – сукупність властивостей системи, які дозволяють довіряти технічній реалізації системи.

Збиток – фактичні або можливі економічні й соціальні втрати спричинені змінами в навколишньому середовищі, що виникають у результаті якихось подій, явищ, дій.

Зловмисник (Intruder) – особа або організація, зацікавлені в отриманні несанкціонованого доступу до програм або даних, роблять спробу такого доступу або вчинили його; порушник, що умисно йде на порушення з корисливих мотивів.

Злом системи – навмисне проникнення в ІС, коли зломщик не має санкціонованих параметрів для входу.

Ідентифікатор (Identifier) – засіб ідентифікації доступу, що є відмітною ознакою суб'єкта або об'єкта доступу. Основним засобом ідентифікації доступу для користувачів є пароль.

Ідентифікація – присвоєння відмітних ознак (спеціальних ідентифікаторів) суб'єктам і об'єктам системи, або порівняння ідентифікатора, що пред'являється, зі збереженим у системі.

Інформаційна безпека – 1) захищеність інформаційного середовища особи, суспільства й держави від зловмисних і незловмисних загроз і впливів; 2) захищеність інформації й

інфраструктури, що підтримується, від випадкових або умисних дій природного або штучного характеру, що можуть завдати збитків власникам або користувачам інформації та інфраструктури.

Інформаційне середовище – сукупність інформаційних ресурсів, систем формування, поширення й використання інформації, інформаційної інфраструктури.

Інформаційні ресурси – задокументована в будь-якій формі інформація, отримана в процесі життєдіяльності громадян, суспільства й держави.

Інцидент інформаційної безпеки – будь-яка подія або сукупність несприятливих подій, що негативно впливає на безпеку мережевих та інформаційних систем, електронних інформаційних ресурсів.

Критерій безпеки – всебічна порівняльна оцінка стану безпеки людини, суспільства, держави й довкілля з погляду найважливіших процесів, явищ, параметрів, що відображають її суть. Критерій є якісною оцінкою, на основі якої адекватно визначається рівень безпеки.

Механізм захисту – засоби захисту, реалізовані для забезпечення служб захисту, необхідних для захисту інформаційної системи.

Модель загроз інформації (Information treats model) – формалізований опис каналів витоку, відомості про методи і засоби здійснення загроз інформації.

Національна безпека – захищеність життєво важливих інтересів особи, суспільства, держави в різних сферах життєдіяльності від внутрішніх і зовнішніх загроз, що забезпечує сталий і поступальний розвиток країни.

Небезпека – постійно присутня в навколишньому середовищі ситуація, що за певних умов може призвести до реалізації небажаної події, з якою пов’язана низка небезпечних для людини, суспільства, держави та довкілля факторів.

Несанкціонований доступ до інформації (Unauthorized access to information), НСД – 1) протиправне навмисне оволодіння конфіденційною інформацією особою, що не має права доступу до відомостей, що охороняються; 2) доступ до інформації, який порушує правила розмежування доступу з використанням штатних засобів, що надаються засобами інформаційної системи.

Нештатна ситуація – ситуація, що виникає в процесі роботи інформаційної системи, але є непередбаченою програмною документацією.

Об’єкт доступу (Access object) – одиниця інформаційного ресурсу, до якої здійснюється доступ штатними програмно-технічними засобами.

Об’єкт захисту – загальний термін для всіх форм існування інформації, що вимагають захисту.

Політика безпеки (Security policy) – набір законів, правил і практичного досвіду, на основі яких будується управління, захист і розподіл критичної інформації.

Порушник – це особа, яка здійснила спробу виконання заборонених операцій (дій) помилково, внаслідок незнання, або усвідомлено зі злим наміром (з корисливих інтересів), або без нього (заради гри або задоволення, з метою самоствердження тощо), і яка використовує для цього різні можливості, методи і засоби.

Ризик – оцінка величини збитку, що може виникати внаслідок ухвалення рішень в умовах невизначеності та реалізації загрози. Ризик є кількісною мірою безпеки, що дорівнює добутку ймовірності реалізації даної загрози на величину можливого збитку від неї.

Спотворення інформації (Distortion) – несанкціонована модифікація інформації при її обробці технічними засобами в результаті зовнішніх дій (перешкод, атак), збоїв в роботі апаратури або невмілих дій обслуговуючого персоналу.

Уразливість (Vulnerability) – властивість системи, яка може привести до порушення її захисту за наявності загрози.

Хакер – 1) професійний висококваліфікований програміст, спроможний, досліджуючи ІС, виявляти слабкі місця (уразливості) у її системі ІБ й інформувати користувачів і розробників системи з метою подальшого усунення знайдених уразливостей. Інше завдання хакера – проаналізувавши існуючу безпеку ІС, сформулювати необхідні вимоги й умови підвищення рівня її захищеності; 2) висококваліфікований програміст, основне завдання якого полягає в тому, щоб несанкціоновано проникати в інформаційні системи із зловмисними цілями (найбільш поширене трактування цього терміну).

Шкідлива програма (Malware) — програма, яка отримує доступ до приватних комп’ютерних систем, перешкоджає роботі комп’ютера або збирає конфіденційну інформацію.

ВСТУП

Інциденти інформаційної безпеки щорічно суттєво зростають, і це зростання сьогодні охоплює навіть ті сфери, які є далекими від ІТ. Водночас виявлення інцидентів досі є занадто повільним.

Особливе занепокоєння викликає той факт, що значна частина атак залишається невиявленою. Як би гарно не зростала кількість технологій захисту, але кількість видів атак завжди є більшою. Постійно зростає і потребує роботи на випередження частка нових невідомих атак, так званих атак «нульового дня». Масштаб проблеми досяг такого рівня, що просто реагувати на інциденти недостатньо. Потрібна система управління безпекою. Без такої системи ми беззахисні перед інформаційними та кібератаками.

В системі управління кібербезпекою суттєве значення має робота на випередження, яка потребує прогнозування розвитку атак та стану безпеки за допомогою математичного моделювання.

Подібно до зростання Інтернету, зокрема у нових формах Інтернету речей (IoT) і Всеохоплюючого Інтернету (IoE), зростає й кількість кібератак. Чим більше вузлів має мережа (кількість з'єднань) тим більше можливостей отримують кіберзлочинці та їх шкідливе програмне забезпечення. Зі збільшенням кількості ланок в мережі зростає схожість закономірностей розвитку кібератак та розвитку біологічних епідемій.

На жаль, традиційні регресійні прогноз-моделі показують лише статистичну інформацію щодо того, що вже відбулось, і не враховують внутрішньої природи джерел небезпеки та цілей інформаційних атак. Однією з перших була виявлена суперечність між вимогами щодо точності прогнозування та якістю вхідних даних. Причому ця суперечна залежність є суттєво нелінійною. Наприклад, при неякісних вхідних даних грубі моделі виявляються більш ефективними.

Отже, завдання вивчення та створення моделей прогнозування кібератак, а також пошуку шляхів контролю розвитку комп'ютерних епідемій є актуальними. Ці завдання вирішуються шляхом розробки прогностичної моделі загроз комп'ютерних вірусів функціонуванню веб-ресурсів органів управління на основі концептуальних підходів, що використовуються у медицині при прогнозуванні розповсюдження захворювань, та за допомогою програмного забезпечення моделювання у середовищі MATLAB.

У розділі 1 проаналізовано стан поширення шкідливих програм у світі і в Україні, наведено опис типів таких програм та їх особливостей. Розглянуті інформаційні небезпеки в мережевому просторі, серед яких найнебезпечнішими є атаки «нульового дня».

У розділі 2 наведено опис засобів захисту від вірусних атак. Для визначення факту та ступеню небезпеки атак, а також для обрання адекватного захисту запропоновано використовувати прогнозування, враховуючи досвід медицини та встановлені аналогії між біологічними епідеміями та кібератаками.

У розділі 3 виявлені поведінкові аналогії біологічних епідемій та кібератак. Зроблений висновок щодо доцільності використання епідеміологічного підходу для моделювання кібератак. Проведено аналіз існуючих моделей епідеміологічного підходу. Проаналізовані вимоги до точності (грубості моделей) залежно від ступеня невизначеності вхідної інформації. За допомогою епідеміологічного підходу створені моделі прогнозування розвитку загроз «нульового дня». Запропонований підхід щодо управління кіберепідемією шляхом утримання її на доепідеміологічному рівні.

Для покращення ідентифікації небезпечних ситуацій шляхом кластеризації потенційних загроз «нульового дня» виконана модифікація таксонометричного методу.

Побудову і використання моделі для всіх етапів здійснено за допомогою пакету MATLAB.

Фотоматеріали, довідкова інформація отримані з різних відкритих джерел Інтернету, яким автори висловлюють свою повагу і шанування.

1 ОПИС ОСНОВНИХ ТИПІВ ШКІДЛИВИХ ПРОГРАМ

«Якщо якась неприємність може статися, вона станеться».

Закон Мерфі

Стан поширення шкідливих програм. Коротка історія шкідливих програм. Типи шкідливих програм. Типи і структура вірусу. Уявлення про схожість поширення комп'ютерних вірусів і біологічних епідемій

1.1. Стан поширення і використання шкідливих програм

Розвиток технологій завжди пов'язаний з небезпеками їх використання. Ця ситуація набула особливого значення з поширенням комп'ютерних технологій, адже їх проникнення охопило практично всі види діяльності. Темпи збільшення інформаційних небезпек упродовж останніх років показують стабільне, більш ніж 65-відсоткове щорічне зростання, що, як мінімум, вдвічі перевищує темпи зростання динамічного ринку мобільних засобів (рис.1.1) [48, 98, 100].

Серед інцидентів кібербезпеки, таких як несанкціонований доступ, крадіжки даних, хакерство, найчастіше загрози надходять від атак щкідливих програм, зокрема вірусів. За даними аналітичних компаній щодня в Іитернеті з'являються десятки тисяч нових зразків шкідливого ПЗ (наприклад, за даними української компанії Zillya! - близько 60 тис. [38]). Цілі таких атак - не просто вивести комп'ютер з

ладу, а нанести економічні збитки, удари по іміджу, сприяти підриву довіри, просуванню потрібного інформаційного контенту.

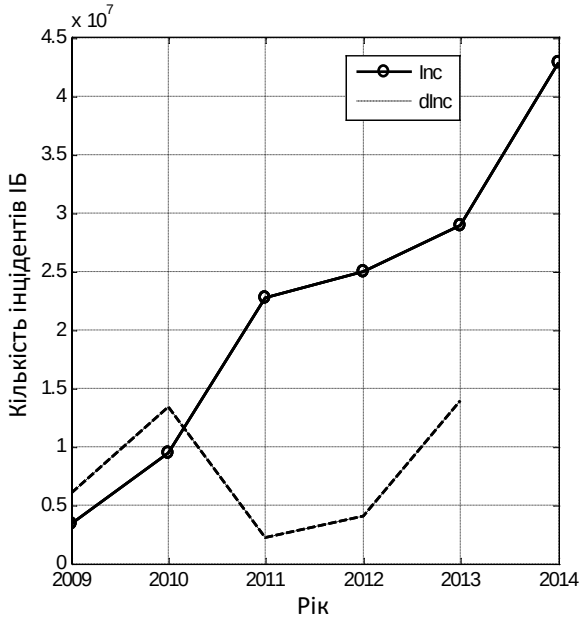


Рис.1.1. Темпи зростання кількості інцидентів ІБ
(Inc – кількість інцидентів ІБ, dInc – щорічний приріст інцидентів ІБ)

Сучасний розвиток інформаційно-комунікаційних технологій, їх широке розповсюдження по усьому світові та технологічні можливості опрацювання значних об'ємів даних дозволили створювати на підприємствах, в установах і організаціях автоматизовані системи різних типів та оприлюднювати інформаційні ресурси в Інтернеті з урахуванням парадигми відкритості діяльності [33]. У зв'язку з цим особливе занепокоєння викликає той факт, що об'єктами посиленої уваги вірусних атак залишаються автоматизовані системи критичних інфраструктур суспільства, зокрема й органів державного управління.

Наприкінці 2016 р. ФБР і Міністерство внутрішньої безпеки США опублікували доповідь про кібератаки російських експертів, метою

яких були об'єкти критичної інфраструктури Америки. Атаки були націлені на урядові установи, наукові інститути і університети, політичні організації і корпорації. Метою атак була крадіжка даних. У доповіді також сказано про атаки на Демократичну партію США. ФБР з'ясувало, що їх виконали упродовж 2015-2016 років під час передвиборної кампанії Клінтон-Трамп дві російські групи хакерів - APT28 (також відома як Fancy Bear) і APT29.

На віртуальному просторі відбилася і війна в Україні. У січні 2015 р. представниками проросійського угрупування «Киберберкут» був зламаний сайт канцлера Німеччини Ангели Меркель. Пізніше атаці і блокуванню піддався сайт тодішнього прем'єр-міністра України yatsenyuk.org.ua.

Таким чином, на сьогодні вже є очевидною глобальна небезпека, на яку наражаються веб-ресурси ОУ у зв'язку із екстенсивним зростанням інцидентів інформаційної безпеки, що призводить до спотворення ресурсів, перешкоджанню діяльності ОУ та погіршенню їх іміджу, особливо у надзвичайних ситуаціях та в критичних сферах, і, як наслідок, до відповідного зниження рівня безпеки ОУ та держави в цілому [16, 32].

Кожного року комп'ютерні віруси причиняють шкоду розміром в декілька мільярдів доларів, викликаючи системні критичні помилки, зупиняючи великі сайти та веб-додатки, знищуючи або модифікуючи файли, підвищуючи час відклику. Ці шкідливі програми крадуть конфіденційну інформацію, розсилають спам з комп'ютерів, користувачі яких нічого не підозрюють, об'єднують ПК з різних куточків світу в ботнети для здійснення DDoS-атак тощо.

За даними щорічного глобального звіту з інформаційної безпеки Security Intelligence Report, опублікованого Microsoft [79], нормами за період лютий 2017 р. - січень 2018 р. стали зловмисні категорії програм, наведені на рис. 1.2, а відсоток поширення шкідливих програм відносно „чистих" комп'ютерів в Україні значно перевищив середньосвітовий рівень (рис. 1.3).

За досить короткий часовий проміжок історії поширення шкідливих програм сформувалась низка гучних подій. Нижче наведено топ-10 програм, згадка про які змушує здригатися простих користувачів і спеціалістів з антивірусної індустрії (за даними українських розробників антивірусних програм Zillya!) [38]. Перелік наведено у порядку зростання величини заподіяної вірусом шкоди.

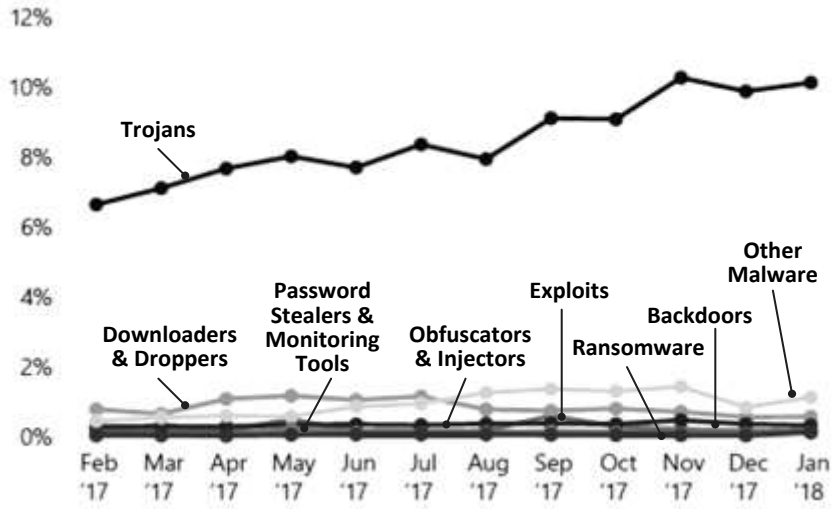


Рис. 1.2. Категорії зловмисних програм, що стали нормою у світі за період з лютого 2017 р. по січень 2018 р.

10. Хробак Морріса. Зразок експерименту, над яким втратили контроль, і це призвело до незапланованих наслідків. У листопаді 1988 року Роберт Морріс вирішив дослідити розміри існуючої на той час комп'ютерної мережі і використав для цього вірус, додавши в нього функцію самокопіювання. Хробак вийшов з-під контролю і спровокував епідемію, заразивши більше 6 000 ПК мережі ARPANET. Збитки від вірусної атаки склали 96,5 мільйонів доларів.

9. Хробак Heartbleed. Шкідлива програма, яка навесні 2014 року змусила хвилюватися весь віртуальний світ. Вірус, випадково створений програмістом Робіном Сеггельменом, використав

уразливості криптографічного пакету OpenSSL і проник за короткий час майже на півмільйона інтернет-сайтів. Heartbleed вкрав особисті дані, інформацію про кредитні карти, паролі у багатомільйонної аудиторії користувачів мережі.

8. Хробак Sasser. Творіння 17-річного школяра з Німеччини розпочало своє поширення мережею навесні 2004 року. Під прицілом вірусної атаки опинилися досить серйозні об'єкти: Британська берегова охорона, авіакомпанія Delta Airlines, інформаційна агенція France-Presse, десятки комп'ютерних мереж великих корпорацій, університетів, лікарень. Збиток від цього вірусу нараховує сотні мільярдів доларів. Але винуватець цих подій, будучи неповнолітнім, так і залишився непокараним.

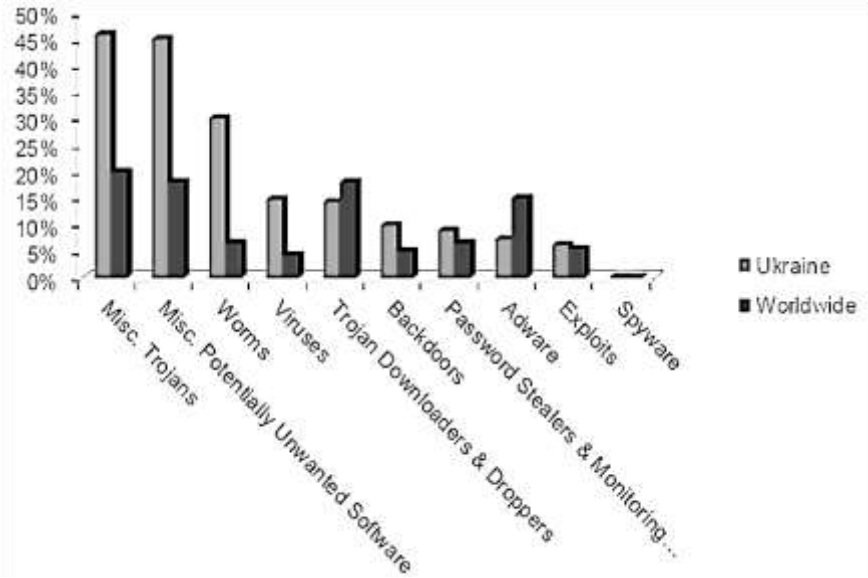


Рис. 1.3. Відсоток поширення зловмисних програм відносно „чистих" комп'ютерів за деякими загрозами в Україні та у світі

7. Вірус WIN.CIH (Чорнобиль). 26 квітня 1999 року на тисячах ПК по всьому світу активізувався вірус, подібних якому ще не було. Використовуючи уразливості ОС Windows 95/98, він через електронну

пошту поширювався від комп'ютера до комп'ютера і пошкоджував вміст жорстких дисків, а подекуди і мікросхеми BIOS. Від вірусу WIN.CIH (Чорнобиль) постраждало 300-500 тисяч ПК, розмір збитків сягає 80 мільйонів доларів.

Автором "Чорнобиля" виявився студент із Тайваню, який розповсюдив вірус в мережі за рік до активації. Це було перше шкідливе ПЗ, яке інфікувало не лише приватні комп'ютери, але й веб-сайти. Прописавшись на ігрових серверах, вірус зміг поширитися у Сполучених Штатах. Але найбільш постраждалим регіоном виявилася Східна Азія.

6. Melissa. В березні 1999 року віртуальний світ вразила епідемія вірусу Melissa, який відносять до категорії мережевих хробаків. Його творець Девід Сміт попередньо розмістив файли з вірусом на деяких форумах у вигляді списку з переліком сайтів для дорослих і паролями доступу до них. Протягом двох днів, використовуючи поштовий сервіс Microsoft Outlook, Melissa поширила свої копії на сотні тисяч ПК. Через вірусну атаку тимчасово були вимушені відключити свої e-mail сервери такі гіганти, як Intel та Microsoft, щоб попередити подальше розповсюдження шкідливої програми. З кожного зараженого комп'ютера вірус розсилав свої копії у вигляді спаму на 50 перших адрес із списку контактів користувача. Таким чином було інфіковано близько мільйона ПК і нанесено збитків на 80 мільйонів доларів.

5. Хробак Stuxnet. Перший хробак-шпигун, який перепрограмовує промислові установки, був використаний для вірусної атаки у 2010 році. В його коді знайдена ділянка, що використовує уразливості операційної системи Windows для отримання доступу до компонентів автоматичної системи управління SCADA. Такі АСУ використовуються на великих ядерних і хімічних підприємствах, на електростанціях і в аеропортах. Stuxnet таємно прописується на деяких програмованих чіпах і може фізично руйнувати інфраструктуру об'єкта.

Авторів вірусу досі не знайдено. Припускається, що це розробка секретних служб деяких впливових держав, і що головною метою цієї шкідливої програми є ядерні заводи Ірану. Результатом діяльності вірусу стало зараження 45 000 комп'ютерних мереж.

4. Code Red. Мережевий хробак Code Red заявив про своє існування влітку 2001 року. Проникаючи на ПК через помилки в ОС Windows, він продовжував пошуки інших вразливих сайтів. За короткий термін (близько 20 днів) вірус інфікував близько 360 000 обчислювальних машин і створив з них зомбі-мережу. Основною метою діяльності хробака була DDoS-атака на веб-сайт Білого Дому. Незважаючи на завдані збитки у розмірі 3 мільярдів доларів, головної мети Code Red досягти не зміг. Причиною стала помилка розробників, особи яких досі не встановлені. Вірусна атака була запланована на IP-адресу, яку вдалося вчасно змінити і зламати плани зловмисників.

3. Slammer. Вірус Slammer став відомий у 2003 році як один з тих, що найшвидше поширюються. Для проникнення на 75 тисяч пристроїв йому знадобилося лише 10 хвилин. Шкідлива програма використовувала одну із уразливостей Windows, про яку було відомо ще за півроку до цього. І Microsoft навіть випустив оновлення, щоб виправити виявлену помилку. Але цей факт проігнорували більшість користувачів, в тому числі і деякі підрозділи самої корпорації.

Швидке розповсюдження вірусу стало можливим завдяки його дуже маленькому об'єму в 376 байт. Slammer поширювався з надзвичайною швидкістю, відправляючи свої копії на випадкові IP-адреси і наповнюючи Інтернет спамовим трафіком. Це викликало значне уповільнення мережі, залишило на деякий час без Інтернету Південну Корею, і вплинуло на роботу системи банкоматів у США. Через деякий час телекомунікаційні канали були переповнені, і атака поступово припинилася.

2. Nimda. Цей багатовекторний мережевий хробак заполонив мережу за короткий проміжок часу восени 2001 року. Усього лише 22 хвилини знадобилося Nimda, щоб проникнути на мільйони комп'ютерів. Для зараження ПК хробак використовував усі доступні шляхи: електронну пошту для розсилки спаму, слабкі місця у захисті ОС, загальнодоступні веб-сайти, навіть знаходив старі бекдори, залишені попередніми вірусами.

1. ILOVEYOU. Єдиний вірус, який було внесено до Книги рекордів Гіннеса як найруйнівнішого у світі. Написаний хакерами з Філіппін, цей хробак у 2000 році інфікував більше 3 мільйонів комп'ютерів по всьому світу і завдав шкоди на 10-15 мільярдів доларів. Для свого поширення ILOVEYOU використовував ті ж схеми, що і Melissa. Але він не лише розсилав свої копії адресатам через Microsoft Outlook, але й поводив себе як типова троянська програма. Він намагався викрасти всі знайдені паролі, які переправляв на поштову скриньку зловмисників. Серед його можливостей було зафіксовано і видалення випадкових файлів з зображеннями або MP3, замість яких записувався вірусний код. ILOVEYOU розмножувався з кожним перезавантаженням Windows.

З роками розвинулась індустрія антивірусного програмного забезпечення, і про вірусні атаки звичайним користувачам хвилюватися можна менше. Сьогодні для них більшу небезпеку становлять трояни, які крадуть конфіденційні дані і залучають комп'ютери до ботнетів. Прогноз розвитку небезпек від компанії Symantec передбачає наступне [71]:

- боти стануть більш складними;
- «штормові хробаки» будуть більш масовими;
- зміцніють загрози веб-застосуванням, оскільки браузери стануть більш уніфікованими в підтримці JavaScript;
- активуються мобільні агенти - програми, які завантажуються на інші комп'ютери й там виконуються (Java-аплети, Active);
- поширяться атаки міжсайтового скриптинга, що дозволяють зловмисникам виконувати шкідливі сценарії від імені довірених веб-сайтів;
- збільшиться число атак на хмари, віртуальні речі з яких можна продати за реальні гроші.

Слід також звернути увагу на два моменти:

- пасивні об'єкти відходять у минуле; активний вміст стає нормою;
- інтеграція різних сервісів, наявність серед них мережних, загальна зв'язність багаторазово збільшують потенціал для атак.

Аналітики групи компаній InfoWatch представили вірогідні сценарії основних кіберзагроз на 2019 р. і позначили найуразливіші напрями з точки зору побудови систем захисту інформаційної безпеки організацій [36], а саме:

- витоків даних стане більше - підвищення рівня цифровізації, формування великих сховищ даних з добре структурованою інформацією, зростаюча цінність різних типів інформації примножують ризики витоків даних;
- державний рівень загроз - тема кібербезпеки міцно увійде до політичного порядку денного багатьох держав;
- головні об'єкти нападу - хакери частіше атакуватимуть великі хмарні сховища даних та фінансову сферу. Використовуючи шкідливе ПЗ, хакери намагатимуться проникнути у банківські мережі з метою компрометації платіжних карток і подальшого виведення великих грошових сум. Досить уразливими перед зловмисниками стають автоматизовані системи управління технологічними процесами. В зоні особливого ризику також знаходяться оператори стільникового зв'язку і компанії сфери електронної комерції;
- атаки на Інтернет речей - зловмисники більш інтенсивно почнуть використовувати уразливості Інтернету речей (IoT) і Індустріального Інтернету (IIoT) у своїх цілях. Підключені пристрої об'єднуватимуть у великі мережі для створення ботнетів, задіюючи їх в DDoS- атаках;
- штучний інтелект - технології штучного інтелекту можуть бути небезпечною зброєю в руках зловмисників. Ймовірно, можливості штучного інтелекту і машинного навчання кіберзлочинці вже в 2019 році почнуть широко використовувати для створення "розумних ботів", націлених на проведення атак;
- шпигунство і удар по брендах - у зв'язку з розвитком конкуренції і наростанням протиріч на міжнародних ринках, підвищується інтерес зловмисників до інформації, що становить ноу-хау і комерційну таємницю.

Компанія Positive Technologies опублікувала дослідження, в якому описані головні тенденції 2017 р. у сфері ІБ [49]. У звіті зазначається, що 13% усіх атак були спрямовані на державні організації, серед об'єктів спрямованості атак 34% склали веб-ресурси (рис. 1.4). Водночас серед методів атак перше місце займає зловмисне ПЗ (39%), а також використання веб-вразливостей - 19% (рис. 1.5).

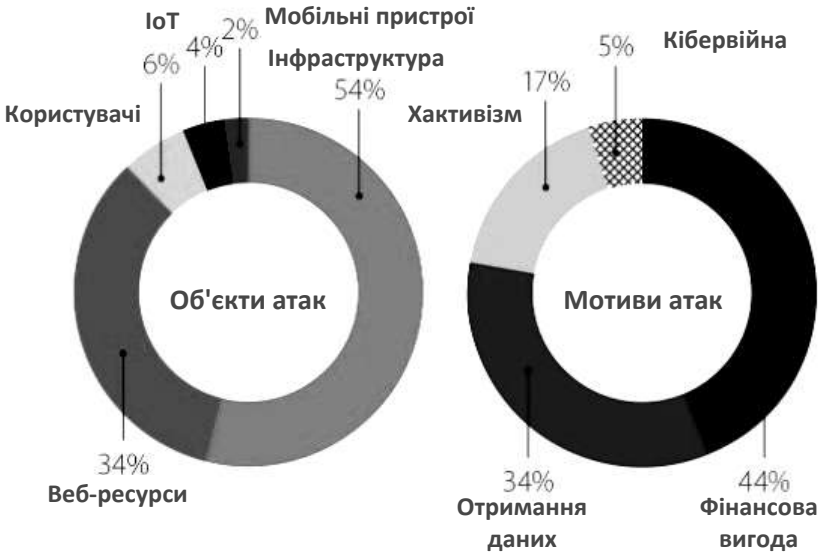


Рис. 1.4. Об'єкти і мотиви атак на державні установи

Як свідчить статистика, зловмисна дія на ресурси АС, зокрема на веб-ресурси, відбувається, як правило, з використанням одночасно кількох різних видів атак. Для зловмисників вірусні атаки — це стаття кримінального кодексу, а для більшості користувачів — це щоденний головний біль і клопіт, причина збоїв у роботі комп'ютера і ворог номер один. Незважаючи на вдосконалення різних методів атак, поширення саме вірусів продовжується. Ось найсвіжіші приклади.

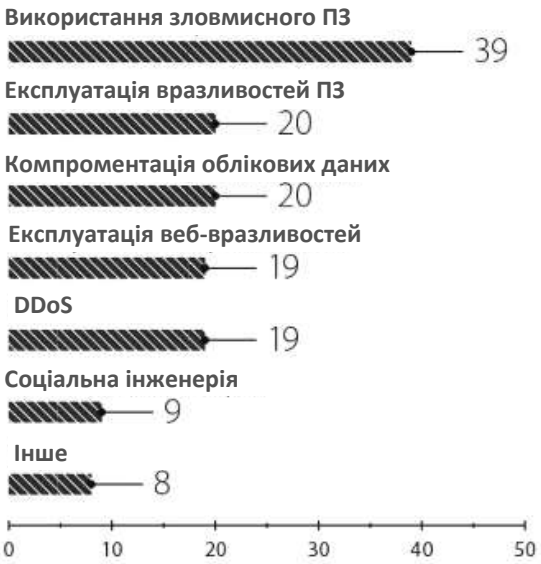


Рис. 1.5. Методи атак на державні установи

У Мережі останнім часом почастішали випадки атак зловмисника-шифрувальника JungleSec. Перші його напади були зафіксовані на початку листопада 2018 р. Примітно, що жертвами атак ставали користувачі систем і Windows, і Mac, і Linux. За даними експертів ресурсу Bleeping Computer, зловмисник в усіх випадках проникав в системи через інтерфейс IPMI (Intelligent Platform Management Interface) - інтерфейс віддаленого управління серверами. Він реалізується через окрему мікросхему, яка може встановлюватися на материнську плату безпосередньо в процесі складання або інсталюватися пізніше. Цей інструмент надзвичайно зручний для системних адміністраторів: він дозволяє, наприклад, віддалено отримувати інформацію про систему, управляти комп'ютерами, вмикати і вимикати їх тощо.

Системи IPMI з помилками конфігурації і незміненим передвстановленим паролем і дозволяють кіберзлочинцям здійснювати атаки через Інтернет. Після зашифровування файлів зловмисник

JungleSec виводить вимогу про сплату викупу за розблокування. Сумна новина полягає в тому, що, за даними Bleeping Computer, жоден з користувачів, що заплатив необхідну суму, досі так і не отримав ключ розшифрування.

27 червня 2017 р. українські державні структури і приватні компанії потрапили під удар "вірусу-вимагача" під назвою Petya.A. Атаці піддалися Кабінет Міністрів, "Ощадбанк", "Укренерго", "Нова пошта", аеропорт Бориспіль, Чорнобильська АЕС й інші організації. Національний банк України констатував, що від кібератаки постраждали близько 30 українських банків.

Потужна хакерська атака почалася з України, а потім поширилась ще на 64 країни світу. Винуватцем зараження експерти назвали програму M.E. Doc, яка використовується в бухгалтерії багатьма українськими організаціями. Була використана уразливість в ОС Windows, так само й у випадку з вірусом WannaCry (також відомий як WannaCrypt), який в травні 2017 р. уразив тисячі комп'ютерів по всьому світові.

Взагалі лише за 2017 р., крім названих, в Україні були виявлені наступні загрози:

Blueborne – уразливість в протоколі Bluetooth;

NotPetya – програма, яка знищує дані на ПК;

KRACK – критична уразливість мереж Wi-Fi;

EternalBlue – програма для одержання віддаленого доступу до системи;

Bad rabbit – вірус-шифрувальник, розроблений для ОС сімейства Windows;

Loki– сімейство шкідливих програм для Android;

Locky – шифрувальник файлів у Windows;

Reaper – вірус, спрямований на IoT-пристрої.

Також наразі в Інтернеті продовжується поширення надзвичайно небезпечного вірусу під назвою WannaCrypt. Зараження вірусом в більшості випадків відбувається через електронну пошту, а також через завантаження файлів з Інтернету. Від більшості шкідливих програм-шифрувальників WannaCry відрізняє подібність характеристик до

мережевого хробака, завдяки яким загроза може самостійно поширюватися. Як результат, шкідлива програма розповсюджується дуже швидко, здійснюючи масове інфікування комп'ютерів користувачів у всьому світі.

Окремою проблемою є постійне зростання кількості виявлених модифікацій зловмисного ПЗ для мобільних пристроїв. 2016 року більш ніж на одному мільйоні мобільних пристроїв на базі Android було виявлено шкідливе програмне забезпечення, яке компанія зі сфери безпеки Check Point назвала Googlian. Вірус використовує уразливості в Android 4 і 5 (Jelly Bean, Kit Kat і Marshmallow) і поширюється в магазинах застосувань. Вірус відразу ж викрадає токен авторизації Google, що дає зловмисникам доступ до акаунту користувача.

2017 року антивірус Dr.Web повідомив про поширення банківської вірусної програми Bankbot, якою заразилися смартфони на Android в десятках країн, у тому числі й в Україні. Троян Android.BankBot.211.origin вимагає від користувачів надати йому доступ до спеціальних можливостей (Accessibility Service). З їх допомогою шкідлива програма управляє мобільними пристроями і краде конфіденційну інформацію клієнтів фінансових організацій. Вірус може демонструвати фальшиві вікна для входу в системи інтернет-банкінгу, платіжні системи і магазин Google Play. Також вірус може викрадати логіни, паролі та іншу автентифікаційну інформацію.

Ці приклади, кількість яких можна множити, свідчать про небезбеку для багатьох сфер суспільства, що поширюється через мобільні пристрої.

Особливо небезпечними є вірусні атаки на об'єкти так званої критичної інфраструктури держави, до якої зазвичай зараховують інфраструктурну сферу (енерго-, тепло-, газопостачання), банківську сферу, сферу телекомунікацій, політичну сферу, оборонну сферу тощо. Вище наводились приклади атак на об'єкти зазначених структур.

2003 року вірус Blaster, також відомий як Lovsan, Lovesan, MSBlaster, викликав відключення світла у Нью-Йорку. 2010 р. через USB був уведений у контролери атомних станцій Ірану вірус Stuxnet,

що зупинив їх функціонування. Хробак начисто знищив на станціях близько 1000 програмованих логічних контролерів від компанії Siemens, що керували поділом урану.

Слід назвати і вже згадану доповідь ФБР і Міністерства внутрішньої безпеки США 2016 року про російські кібератаки, націлені на об'єкти критичної інфраструктури держави, зокрема на урядові установи, наукові інститути і університети, політичні організації і корпорації.

Інциденти з відключенням електроенергії у Києві у 2015-2016 роках, що зачепили сотні тисяч жителів столиці, є наслідком хакерських атак. У цьому переконані фахівці компанії з кібербезпеки Information Systems Security Partners (ISSP). Зломи енергомережі пов'язані між собою і ще з декількома хакерськими атаками на системи державних органів (залізниця, міністерства, пенсійний фонд).

Вивчення інцидентів в межах критичних інфраструктур свідчить про значний відсоток атак високої і середньої складності, реагування на які без випереджувальних заходів є малоефективним (рис. 1.6).

Рис. 1.6. Рівні складності кібератак на критичні інфраструктури суспільства

Через значне збільшення інтернет-активності як організацій, так і окремих осіб, а також розвиток Інтернету речей і хмарних технологій атаки можуть бути спрямовані на все що завгодно, при цьому будь-який засіб може стати зброєю. Поки ще захист IoT-пристроїв для їх виробників залишається другорядним питанням. Коли мова йде про викрадення дрону або злом «розумної» кавоварки, це одне, але з масовим впровадженням таких технологій в рази зростає загроза і для життя людини. Наприклад, отримання віддаленого доступу до кардіостимулятора або автомобіля з безпілотним управлінням може призвести до летального результату.

Враховуючи такі обставини Агентство Європейського союзу з мереж і інформаційної безпеки (ENISA) вже внесло інциденти з IoT-пристроями до трійки загроз з найбільшим фінансовим збитком для компаній.

При цьому загрози стають усе більш витонченими, вони можуть функціонувати автономно, і виявити їх все важче. Останньою тенденцію є повернення старих загроз, зокрема тривіальних вірусів, вдосконалених за допомогою нових технологій. Все це відкриває нові горизонти у сфері виявлення і аналізу загроз, а також їх попередження.

1.2. Коротка історія шкідливих програм

Поняття «комп'ютерний вірус» *(computer virus)* з'явилося на початку 1970-х і походить від однойменного терміну з біології через спроможність комп`ютерних вірусів до саморозмноження. Воно згадується у фантастичному оповіданні «Людина в рубцях» Грегорі Белфорда. Ідею створення комп'ютерних вірусів окреслив письменник-фантаст Т. Дж. Райн, який в одній із своїх книжок (1977 р.) описав епідемію, що за короткий час охопила близько 7000 комп'ютерів. У професійних колах термін «комп'ютерний вірус» з'явився у 1984 році, коли його вперше вжив на конференції співробітник Лехайського університету (США) Фред Коен (Fred Cohen).

За означенням Коена «комп'ютерний вірус - це програма, що має здатність заражати інші програми шляхом додавання до них своєї, можливо зміненої, копії». Означення це є доволі неоднозначним, і чіткого формального визначення, що ж таке комп'ютерний вірус, немає й до цього часу. Єдине, що необхідно відмітити, це те, що комп'ютерний вірус – це програма, здатна до відтворення самої себе.

Перші дослідження подібних штучних конструкцій проводились ще в середині минулого століття відомими вченими-математиками Джоном фон Нейманом і Норбертом Вінером. Одним з напрямків таких досліджень було вивчення самовідтворювальних кінцевих автоматів.

Отже, програми, здатні до відтворення самих себе, назвали вірусами за аналогією до біологічних вірусів, що викликають хвороби. Щоб розвиватися, біологічному вірусу необхідний живий організм, в якому він буде створювати свої копії. Так і комп'ютерному вірусу для розмноження необхідно потрапити у програмне середовище комп'ютера і надалі заражати його якомога більше.

Головною умовою існування вірусів є універсальна інтерпретація даних в обчислювальних системах. Один і той самий вірус у процесі зараження програми може сприймати її як дані, а в процесі виконання - вже як виконавчий код. Цей принцип було покладено в основу всіх сучасних комп'ютерних систем, які використовують архітектуру фон Неймана.

Першими вірусами можна вважати програмки, здатні робити копії самих себе, які у 1961 році розробили інженери Віктор Висоцький, Дуг Макілрой і Роберт Морріс з фірми Bell Telephone Laboratories. Вони були створені у вигляді гри, яку інженери назвали «Дарвін». Метою гри було відправляти ці програми друзям, щоб подивитися, яка з них знищить більше програм опонента і зробить більше власних копій. Гравець, якому вдавалося заповнити комп'ютери інших, оголошувався переможцем.

У 1981 Річард Скрента написав один з перших завантажувальних вірусів для ПЕОМ Apple II — ELK CLONER. Він виявляв свою присутність повідомленням, що містило навіть невеликий вірш.

Черговим етапом вважається 1987 рік. До цього моменту отримали широке розповсюдження порівняно дешеві комп'ютери IBM PC, що призвело до різкого збільшення масштабу зараження комп'ютерними вірусами. Саме у 1987 році спалахнули відразу три крупні епідемії.

Наприкінці 1989 р. в пресі з'явилося повідомлення про виявлення в Японії нового, надзвичайно підступного і руйнівного вірусу (його назвали хробаком). За короткий час він знищив дані безлічі комп'ютерів, під'єднаних до комунікаційних ліній.

У 1992 році з'явився перший конструктор вірусів для персональних комп'ютерів IBM PC — Virus Creation Laboratory (для ПК Amiga конструктори існували і раніше), а також готові поліморфні модулі (MtE, DAME і TPE) і модулі шифрування для вбудовування в нові віруси. Протягом кількох наступних років було остаточно відточено стелс і поліморфні технології (SMEG.Pathogen, SMEG.Queeg, OneHalf, NightFall, Nostradamus, Nutcracker), а також випробувано наднезвичайні способи проникнення в систему і зараження файлів (Dir II, PMBS, Shadowgard, Cruncher). Крім того, з'явилися віруси, що заражають об'єктні файли (Shifter) і вихідні тексти програм (SrcVir).

З розповсюдженням пакету Microsoft Office набули поширення макровіруси (Concept). У 1996 році з'явився перший вірус для Windows 95 — Win95.Boza, а в грудні того ж року — перший резидентний вірус для неї — Win95.Punch. З поширенням мереж та Інтернету файлові віруси дедалі більше стали орієнтуватися на них як на основний канал роботи (ShareFun — макровірус MS Word, що використовує MS-Mail для поширення, Win32.HLLP.DeTroie — сімейство вірусів-шпигунів, Melissa — макровірус і мережевий хробак, який побив усі рекорди за швидкістю поширення). Еру розквіту «троянських коней» відкриває у 1998 р. утиліта прихованого віддаленого адміністрування Back Orifice і аналоги, що пішли за нею (NetBus, Phase). Вірус Win95.CIH досяг апогею в застосуванні незвичайних методів, переписуючи BIOS заражених комп'ютерів (епідемія в червні 1998 вважається найбільш руйнівною за попередні роки).

1.3. Типи шкідливих програм

На жаль, на сьогодні віруси створюються вже не групкою ентузіастів і зовсім не для іграшок. Більш того, сформувалась ціла індустрія розробки і використання різних шкідливих програм.

Майже всі сучасні реалізації створюються зловмисниками, які мають на меті роздобути конфіденційні дані користувача або використовувати його комп'ютер в особистих цілях, зокрема комерційних. Фінансовий оборот комп'ютерної мафії вже порівнюють з капіталами наркоторгівлі.

Розглянемо основні типи шкідливих програм. За механізмом поширення і дії розрізняють такі зловмисні програми, як власне віруси (*virus*), а також хробаки (*worm*), троянські (*trojan*), експлойти (*exploit*), шпигунські (*malware*) і рекламні (*adware*) програми. Існують також і змішані конструкції.

Власне *віруси* вирізняються тим, що являють собою код, який має здатність до поширення (можливо, зі змінами) шляхом копіювання свого тіла або вбудовування його в код інших програм (прикріплення до них). На відміну від хробаків, віруси поширюються серед локальних ресурсів комп'ютера і не використовують мережевих сервісів для свого розмноження. Копії заражених програм, передаючись через зовнішні цифрові носії (USB-Flash, CD-диски) або мережею на інші комп'ютери, призводять до масових вірусних епідемій.

Хробак - це програма, яка може використовувати різні методи розповсюдження: самостійно (звичайний хробак), або використовуючи агента-користувача (поштовий хробак). Більшість створених комп'ютерних хробаків спрямовані на розповсюдження, і майже завжди завдають шкоди мережі, наприклад, споживаючи її пропускну здатність. Хоча хробак також робить копії самого себе, але він не може стати частиною іншої нешкідливої програми. Класифікація хробаків [89] наведена на рис. 1.7, а класифікація атак хробаків – на рис. 1.8.

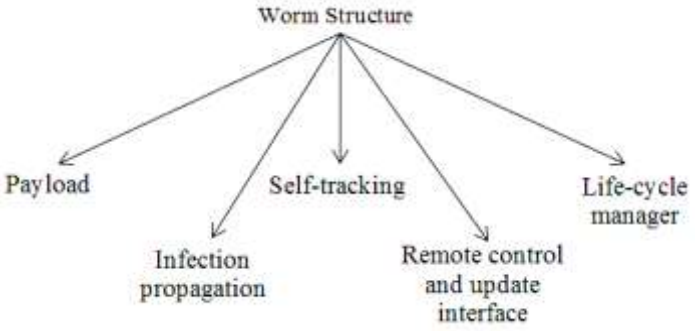


Рис. 1.7. Класифікація хробаків

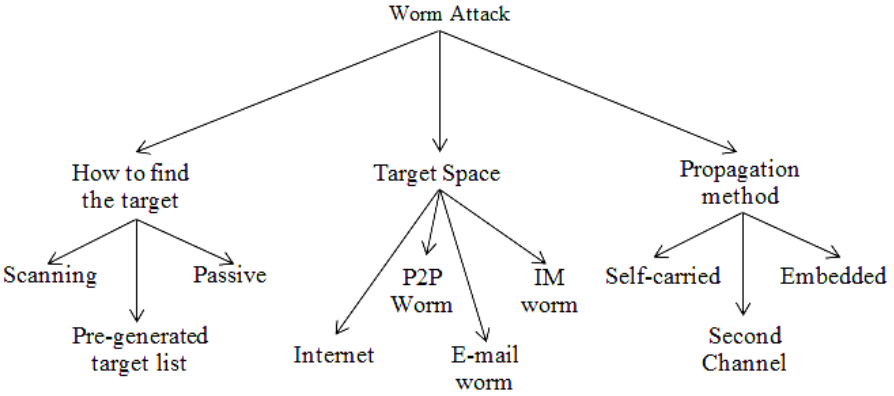


Рис. 1.8. Класифікація атак хробаків

Троянська програма є найнебезпечнішим типом, оскільки вона маскується в інших нешкідливих програмах. Тобто це шкідливий код, що має вигляд функціонально корисної програми. І до того моменту, поки користувач не запустить цю нешкідливу програму, троян не несе ніякої небезпеки і виявити його нелегко. Троянська програма може спричинити різну шкоду для власника комп'ютера. В основному трояни використовуються для крадіжки, зміни або видалення особистих даних

користувача. Відмінною принциповою особливістю троянa є те, що він не може самостійно розмножуватися, у той час як вірус після попадання в комп'ютерну систему існує автономно і в процесі свого функціонування заражає (інфікує) програми.

Віруси можуть використовуватись інтегровано з іншими зловмисними програмами. Так віруси-маскувальники (*Rootkit*) використовуються для приховування шкідливої активності. Вони маскують шкідливі програми, щоб уникнути їх виявлення антивірусами. Руткіти також можуть модифікувати операційну систему на комп'ютері й замінювати основні її функції, щоб приховати власну присутність і дії, які робить зловмисник на зараженому комп'ютері.

Інша реалізація – це зомбі (*Zombie*). Віруси зомбі дозволяють зловмисникові керувати комп'ютером користувача. Комп'ютери-зомбі можуть бути об'єднані в мережу (ботнет) і використовуватися для масової атаки на сайти, розсилання спаму або для інших злочинних дій. Ботнет (*botnet* від *robot* і *network*) – мережа, що складається з деякої кількості хостів із активованими ботами – автономним ПЗ (рис. 1.9). Бот приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Користувач може навіть не здогадуватися, що його комп'ютер зомбований і використовується зловмисником.

Ще одна реалізація - спеціальні хакерські утиліти експлойти (exploit) – пакети шкідливих програм, що використовуються для організації автоматичних (drive-by) атак з метою поширення шкідливого ПЗ або порушення роботи (рис.1.10, 1.11). Набори експлойтів націлені на уразливості найуживаніших офісних застосувань.

Програми-шпигуни (spyware) збирають інформацію про поведінку і дії користувача. Шпигунське ПЗ може записувати все, що набирається на клавіатурі, або контролювати всі сторінки, переглянуті в браузері, і замінювати банерну рекламу на іншу. Здебільшого ці програми спрямовані на отримання інформації про адреси, паролі, дані кредитних карт.

Рис. 1.9. Принцип дії ботнету та цілі його впливу

Рис. 1.10. Чинники, що призводять до атак drive-by через Інтернет із завантаженням шкідливих програм

Жадібні програми (greedy programs) намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використати його. Безпосередній атаці в більшості випадків піддаються

такі об’єкти системи, як процесор, оперативна память, пристрої введення-виведення.

Критична ситуація може виникнути тоді, коли "жадібна" програма виконує нескінчений цикл. Оскільки в багатьох ОС час використання процесора для однієї програми є обмеженим і контролюється системою, то "жадібна" програма може перехоплювати асинхронне до основної програми повідомлення про закінчення операцій введення-виведення і посилати запит на нове введення. Так можна досягти зациклення без можливості втручання ОС. Такі атаки називають також асинхронними. Інший варіант "жадібної" програми - захоплення дуже великої ділянки оперативної пам’яті. Це є можливим, наприклад, при послідовному розміщенні в ОП великого обсягу даних, що надходять із зовнішнього носія (забивання пам’яті).

Рис. 1.11. Схема атаки експлойту із завантаженням шкідливого виконуваного файлу

Нарешті, дуже популярним стало використання соціальних методів, зокрема тактик обману, схожих на маркетингові акції, рекламного програмного забезпечення, фішингу з використанням

соціальних мереж для запотягу користувачів, а також застосування шахрайського ПЗ для забезпечення безпеки, що має назву «scareware» (від англ. scare - лякати).

Програми-реклами (adware) без відома користувачів вбудовуються в різне програмне забезпечення, як правило таке, що поширюється безкоштовно, з метою демонстрації рекламних оголошень. Реклама розташовується в робочому інтерфейсі. Найчастіше такі програми також збирають і переправляють своєму розробникові персональну інформацію про користувача, зокрема про його звички використовувати інтернет-ресурси.

Інший різновид - блокувальники (winlock). Такі програми блокують користувачеві доступ до операційної системи. При завантаженні комп'ютера з'являється вікно, в якому користувача звинувачують у скачуванні неліцензійного контенту або порушенні авторських прав. І під загрозою повного видалення всіх даних з комп'ютера вимагають відіслати смс на номер телефону або поповнити його рахунок. Звісно, що після переказу грошей на рахунок зловмисника банер нікуди не зникає.

Популярність того чи іншого виду шкідливих програм можна проілюструвати їх рейтингами в англомовній науково-технічній літературі (рис. 1.12).

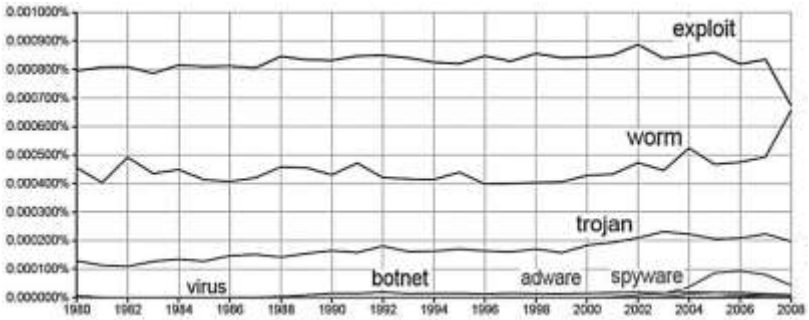


Рис. 1.12. Рейтинги деякого шкідливого ПЗ в англомовній науково-технічній літературі за період 1980-2010 рр. (за даними Google books Ngram Viewer)

1.4. Види і структура вірусу

Як не існує однозначного визначення комп'ютерного вірусу, так немає і єдиної системи класифікації та іменування вірусів (хоча перші спроби створити стандарт були здійснені ще у 90-х роках минулого століття). Тому існують різні підходи до класифікації вірусів.

Виходячи з різних способів поширення розрізняють віруси:

- файлові;
- завантажувальні;
- макровіруси;
- скриптові віруси.

Файлові віруси (File infectors) – вид комп'ютерних вірусів, що розмножуються, використовуючи файлову систему шляхом запису свого коду в код виконуваного файлу конкретної операційної системи. До типів файлів, що потенційно можуть бути інфікованими, належать бінарні файли .exe та .com; файли динамічних бібліотек .dll; драйвери .sys; командні файли .bat, .cmd тощо.

Окремо слід виділити інші види вірусів, що розповсюджуються файловою системою за допомогою файлів інших типів (офісні, пакетні, тощо). Зокрема, до таких можна віднести макровіруси.

Завантажувальний вірус, або вірус завантажувального сектора (Boot-sector virus) – комп'ютерний вірус, що записується в завантажувальний сектор жорсткого диску чи флеш-накопичувача й активізується при завантаженні комп'ютера. При звертанні до нового диска, вірус копіює себе в його завантажувальний сектор і таким чином заражає його. Через специфіку архітектури персональних комп'ютерів типу IBM PC навіть носій, що не є системним, містить бут-сектор.

Скриптовий вірус – це комп'ютерний вірус, написаний мовами Visual Basic, Basic Script, Java Script та подібними скриптовими мовами. На комп'ютер користувача такі віруси, частіше за все, проникають разом з поштовими повідомленнями, що містять у їх вкладеннях файли-

сценарії. Програмний код вірусу також може бути вбудований безпосередньо у HTML-документ і в такому випадку інтерпретуватися браузером.

Зазначені види вірусів можуть перетворюватись на вірус-невидимку, або стелс-вірус (Stealth virus), повністю або частково приховуючи свою присутність в системі шляхом перехоплення звернень до операційної системи, що здійснює читання, запис, читання додаткової інформації про заражені об'єкти (завантажені сектори, елементи файлової системи, пам'яті і т.ін.). Першим стелс-вірусом прийнято вважати вірус Frodo (1987 р.). Вірус умів замінювати заражену ділянку незараженим оригіналом в моменти звернення до нього антивірусної програми. Через таку оригінальність антивірусні програми досить довгий час не могли знешкодити його. Тому це спричинило невелику вірусну епідемію. До відомих Stealth-вірусів належать такі: Virus.DOS.Stealth.551, Exploit.Macro.Stealth, Exploit.MSWord.Stealth, Brain, Fish # 6.

Віруси-примари маскуються за допомогою іншого механізму. Ці віруси постійно модифікують себе таким чином, що не містять однакових фрагментів. Такі віруси зберігають своє тіло в закодованому вигляді і постійно змінюють параметри цього кодування.

Однією з технологій приховування є використання поліморфного коду, котрий може себе змінювати без зміни свого алгоритму. Код може змінюватися кожного разу під час виконання, але результат роботи ніколи не змінюється. Дана техніка породила так звані поліморфні віруси. Ця технологія використовується для того, щоб ускладнити процес пошуку вірусу антивірусними програмами, адже поліморфні віруси не мають постійних пізнавальних груп - сигнатур.

За способом зараження місця існування комп'ютерні віруси поділяються на:

- резидентні;
- нерезидентні.

Резидентні віруси після їх активізації повністю або частково переміщуються з місця існування (мережа, завантажувальний сектор,

файл) в оперативну пам'ять комп'ютера. Ці віруси, використовуючи, як правило, привілейовані режими роботи, дозволені тільки операційній системі, заражають місце існування і при виконанні певних умов реалізують деструктивну функцію. На відміну від резидентних нерезидентні віруси потрапляють в оперативну пам'ять комп'ютера тільки на час їх активності, протягом якого виконують деструктивну функцію і функцію зараження. Потім віруси повністю покидають оперативну пам'ять, залишаючись в місці існування. Якщо вірус розміщує в оперативній пам'яті програму, яка не заражає місце існування, тоді такий вірус вважається нерезидентним.

Існує також класифікація, в якій назва вірусу відображає ту чи іншу його властивість, а саме:

- за місцем виявлення або розробки вірусу;
- за змістом текстових рядків у коді вірусу;
- за ефектом дії вірусу;
- за довжиною вірусу або зростанням довжини файлу при зараженні;
- за датою активації.

В процесі виконання своїх дій кожен вірус створює в комп'ютерній системі низку притаманних саме йому ефектів, які однозначно вказують на його присутність:

- спотворення інформації у файлах або таблиці розміщення файлів (FAT);
- імітація порушень в роботі апаратного забезпечення;
- створення звукових і візуальних ефектів, наприклад, сигнали точного часу через кожну годину або віконечко з деяким написом;
- повідомлення неправдивого змісту про стан системи, що ускладнюють роботу користувача;
- ініціювання помилок в програмах або ОС;
- зчитування даних з пам'яті і переміщення їх в інше місце.

Що стосується фізичної структури вірусу, то вона є доволі простою і складається з голови та тіла (хвоста). Голова - це та частина коду вірусу, що виконується першою. Код тіла розміщується окремо від

голови в коді зараженої програми. Якщо вірус складається лише з голови, тоді він називається несегментованим, якщо з голови та тіла – сегментованим.

Для зараження файлів віруси використовують три основних способи (рис.1.13):

- запис з перекриттям (*overwriting*),
- запис на початку (*prepending*),
- запис в кінці файлу (*appending*).

Рис. 1.13. Варіанти розміщення вірусу у коді програми

В першому випадку файл виявляється повністю зіпсованим, оскільки частину даних було затерто вірусом. Такі віруси зустрічаються вкрай рідко. При спробі відкрити заражений файл відбувається зараження ще одного файлу. Коли вірус записує себе на початку файлу, при його відкритті першим запускається код вірусу, а потім програма-оригінал. Віруси, розміщені після основного коду, переміщують початок програми в кінець файлу, а на його місці розміщують команду переходу на початок завантаження (jmp). Тобто керування одразу передається вірусу, який здійснює перенос початку програми назад і дозволяє програмі запуститись.

З поняттям "комп'ютерний вірус" також тісно пов'язане таке поняття, як сигнатура. Сигнатура - це фрагмент коду, який є у всіх

копіях вірусу, і тільки в них. Тобто це є підписом вірусу, що однозначно позначає його присутність або відсутність у програмі. Ця характерна ознака вірусу використовується для його виявлення більшістю сучасних антивірусних засобів. Метод виявлення, що базується на сигнатурах полягає у тому, що програма-антивірус, переглядаючи файл, звертається до словника з відомими сигнатурами вірусів, складеного авторами програми. У разі відповідності будь-якої ділянки коду програми, яка переглядається, відомому коду (сигнатурі) вірусу в словнику, антивірус може здійснити виконання передбачених дій.

Будь-який вірус, незалежно від приналежності до певних класів, повинен мати три функціональні блоки: блок зараження (розповсюдження), блок маскування і блок виконання деструктивних дій. Розділення на функціональні блоки означає, що до певного блоку належать команди програми вірусу, що виконують одну з трьох функцій, незалежно від місця розташування команд в тілі вірусу.

Після передачі управління вірусу, як правило, виконуються певні функції блоку маскування. Наприклад, здійснюється розшифруваннння тіла вірусу. Потім вірус здійснює функцію впровадження в незаражене місце існування. Якщо вірус призначений для деструктивних дій, то вони можуть здійснюватись або безумовно, або при виконанні певних умов.

Завершує роботу вірусу завжди блок маскування. При цьому можуть виконуватись, наприклад, такі дії: шифрування вірусу (якщо функція шифрування реалізована), відновлення старої дати зміни файлу, відновлення атрибутів файлу, коректування таблиць ОС та ін.

В останню чергу запускається команда переходу на виконання заражених файлів або на виконання програм ОС.

1.5. Уявлення про схожість поширення комп'ютерних вірусів і біологічних епідемій

Попереднє вивчення стану проблеми вірусних атак у комп'ютерній сфері виявило, що їх поширення за своєю природою має багато спільного з біологічними епідеміями. Було визнано, що результати вивчення закономірностей біологічних епідемій, накопичені протягом багатьох століть, можуть бути корисними для аналізу розвитку кібератак. Це, у свою чергу, дозволило, зокрема для прогнозування стану інформаційної безпеки, запропонувати епідеміологічний підхід [25].

Не буде перебільшенням зазначити, що історія людства – це історія епідемій [23]. Серед найвідоміших фактів, що підтверджують цю тезу, можна назвати епідемію віспи 480 р. до н.е., яка вирішила долю протистояння Персів та Греків на користь останніх, «юстіанову чуму» 6-го століття у Візантії (за 50 років померло близько 100 млн.чол.), епідемію бубонної чуми 14-го сторіччя (померла третина населення Азії та половина населення Європи), грип «іспанка» у 1918 році (забрав декілька десятків мільонів життів) [19].

Епідемією (грец. ἐπιδημία - поголовна хвороба серед народу) з давніх часів називають захворювання, яке прогресує у часі і просторі і перевищує звичайний рівень захворюваності на певному терені. Масштабність епідемій призводить до пандемій – таких епідемій, що поширюються на території цілої країни, декількох країн або іноді навіть й за межами одного континенту. Це хвороби, які набули масового характеру і вразили значну кількість населення планети. Напиклад, найбільшою і найвідомішою пандемією чуми була "чорна смерть" 1346-1353 років. Джерелами епідемії були Кітай та Індія, а до Європи хвороба дійшла з монгольськими військами і торговими караванами. Тоді загинуло не менше 60 мільйонів людей.

Сер Рональд Росс (1857 — 1932) — видатний британський лікар паразитолог шотландського походження, лауреат Нобелівської премії з фізіології та медицини у 1902 р. за дослідження малярії

Масштабність епідемій призвела до високого рівня системності дій лікарів. Але, незважаючи на успіхи сучасної медицини, питання протидії епідеміям залишається актуальним [45]. Тому при вивченні закономірностей інфекційних хвороб широко використовують математичні методи досліджень епідемій. Першопрохідцями в моделюванні інфекційних захворювань були Вільям Хамер (William Hamer) та Рональд Росс[1] (Ronald Ross). На початку XX століття Хамер опублікував роботу Epidemiology Old and New (1928), і спільно з Россом вони застосували закон дії мас, щоб пояснити поведінку епідемії. Лоуелл Рід (Lowell Reed) і Уейд Хемптон Фрост (Wade Hampton Frost) розробили епідемічну модель Reed-Frost, щоб описати зв'язок між сприйнятливими до захворювання, інфікованими і такими особинами в популяції, які набули імунітету. Практично у той же час була запропонована модель Kermack-McKendrick - гіпотеза, яка прогнозує кількість і поширення випадків інфекційної хвороби у зв'язку з її передачею серед населення протягом певного часу. Ця модель епідемії передбачила поведінку спалахів, дуже подібних до тих, що спостерігалися у багатьох записаних епідеміях.

Сучасна епідеміологія базується на системному підході й приділяє велику увагу прогнозуванню можливих варіантів розвитку епідемій для вчасного прийняття адекватних протиепідемічних заходів.

Одним із найвідоміших прикладів такого підходу є створення сервісу Google Flu Trends для прогнозування поширення зимового

[1] Фото: автор: невідомий - https://ihm.nlm.nih.gov/images/B22803, Суспільне надбання (Public Domain), https://commons.wikimedia.org/w/index.php?curid=108775

грипу в США (рис. 1.14). У 2009 році був виявлений новий штам вірусу грипу — H1N1, який швидко поширився і в лічені тижні викликав в установах охорони здоров'я по всьому світу побоювання, що насувається страшна пандемія, адже проти нового вірусу не було вакцини.

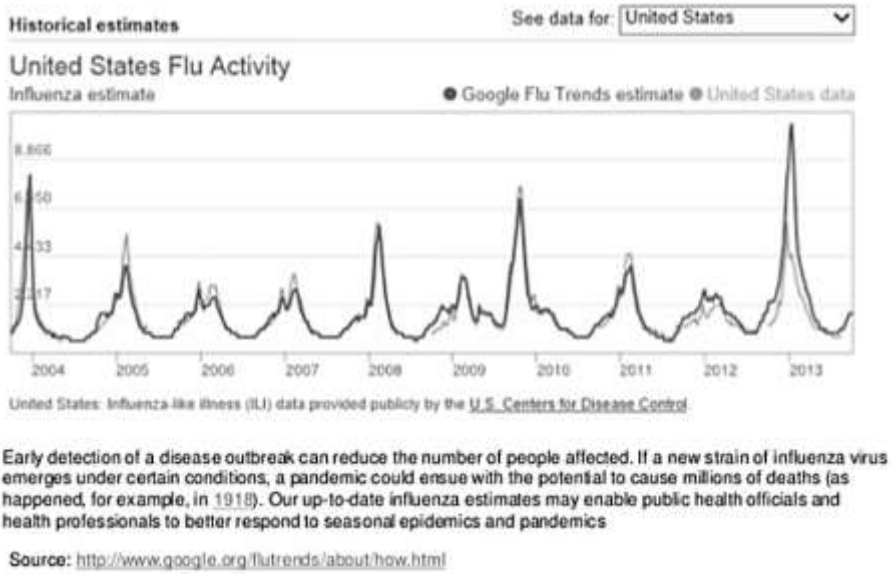


Рис. 1.14. Сторінка Google з оцінками розвитку грипу в США

У США, як і в інших країнах, центри з контролю і профілактики захворювань (Centers for Disease Control and Prevention - CDC) зобов'язали лікарні повідомляти про нові випадки грипу. І все ж таки інформація про захворювання, що виникали кожного разу, запізнювалася на один-два тижні. Але за декілька тижнів до того, як відомості про H1N1 попали на перші смуги газет, інженери Google опублікували статтю в науковому журналі Nature, у якій йшлося про те, як Google може «передбачити» поширення грипу в США не лише в масштабах країни, але і в окремих регіонах і штатах.

Щоб досягнути такого результату, фахівці Google проаналізували пошукові запити інтернет-користувачів. Більше трьох мільярдів запитів, що відправляються в пошукову систему Google щодня зі всього світу, склали величезний масив даних для обробки. 50 мільйонів найбільш поширених умов пошуку, які використовують американці, були порівняні з даними CDC про поширення сезонного грипу в період між 2003 і 2008 роками. Ідея полягала в тому, що людей, що підхопили вірус грипу, можна визначити по тому, що вони шукають в Інтернеті. Була розроблена універсальна система, дія якої зводилася до того, щоб знаходити кореляції між частотою певних пошукових запитів (наприклад, «засіб від кашлю і температури») і поширенням грипу в часі і просторі.

В цілому пошукова система Google провела приголомшливу кількість обробок (450 мільйонів) різних математичних моделей з метою перевірки умов пошуку. Фахівці Google і їх програмне забезпечення виявили поєднання 45 умов пошуку, використання яких у математичних моделях давало коефіцієнт кореляції між прогнозованими і офіційними даними на рівні 97%. Важливо, що компанія змогла назвати територію поширення грипу практично в режимі реального часу.

Отже, чимало фахівців стверджують, що комп'ютерні віруси діють аналогічно до біологічних, і, відповідно, між біологічними епідеміями та поширенням комп'ютерних вірусів є чимало спільного. Так, наприклад, у табл. 1.1 наведено порівняння передумов виникнення біологічних і комп'ютерних епідемій, при інтенсивній дії яких відбувається старт епідемії, а у табл. 1.2 - чинників, що сприяють її розвитку. Нарешті, очевидно, що запобігання виникненню і поширенню чинників, що сприяють розвитку епідемії, уповільнює передачу інфекції, тобто зменшує ризики розвитку епідемій – як біологічних, так і комп'ютерних.

Таблиця 1.1

Передумови виникнення епідемій	
біологічних	**комп'ютерних**
наявність активних джерел інфекції	наявність хоча б одного джерела інфекції
відсутність активного спротиву реалізації механізмів і шляхів передачі	теж саме
наявність переносників	теж саме
наявність сприйнятливого населення	наявність незахищених об'єктів в мережі (комп'ютерів)
порушення санітарних правил	недотримання правил «комп'ютерної гігієни»
недостатня профілактична робота органів охорони здоров'я	недостатня ефективність політики безпеки

Таблиця 1.2

Чинники, що сприяють розвитку епідемії	
біологічних	**комп'ютерних**
велика щільність населення на даній території	велика щільність комп'ютерів на даній території
наявність природних вогнищ інфекцій, які передаються комахами	наявність розвинутих мережевих з'єднань
рухливість місцевого населення	активність використання комп'ютерів користувачами
недостатність комунального благоустрою і скупченість в оселях	наявність незахищених локальних мереж комп'ютерів
порушення санітарного режиму праці на виробництві	недотримання правил «комп'ютерної гігієни»
недостатній рівень санітарної культури населення	брак відповідних знань у користувачів
погана організація вакцинації або неможливість здійснення масової специфічної профілактики (відсутність ефективних засобів специфічної профілактики при ряді інфекційних хвороб, відсутність або недостача препаратів для масової профілактики)	недостатня ефективність політики безпеки, невиконання заходів програми безпеки, зокрема щодо впровадження антивірусних засобів
незадовільна організація клінічної, лабораторної та санітарно-протиепідемічної допомоги населенню	незадовільна організація просвітнього і правового забезпечення користувачів

Найбільш цікавим з точки зору порівняння є епідемічний процес як безперервна взаємодія на видовому і популяційному рівнях між неоднорідними за еволюційно-зв'язаними ознаками стосовно один одного збудником-паразитом і біологічним організмом в необхідних і достатніх соціальних і природних умовах.

Відповідно до закону, виведеному Л. В. Громашевським[2], епідемічний процес розвивається по тріаді:

- джерело збудника інфекції;
- механізм передачі збудника інфекції;
- сприйнятливий організм.

У табл. 1.3 наведено порівняння прийнятої у біології термінології епідемічного процесу з відповідними визначеннями з комп'ютерної сфери, а у табл. 1.4 – порівняння періодів епідемічного процесу.

Ці таблиці підтверджують суттєву спільність між біологічними епідеміями та поширенням комп'ютерних вірусів. Водночас необхідно зазначити, що, зрозуміло, між ними є й певні відмінності.

Лев (Левко) Васильович Громашевський (1887 — 1980) — видатний український радянський епідеміолог, розробник вчення про механізми передачі інфекції, автор оригінальної класифікації інфекційних хвороб, академік АМН СРСР, Заслужений діяч науки УРСР, Герой Соціалістичної Праці

Збудниками біологічних епідемій можуть бути не лише віруси, але й мікроби. Обидва паразитують на клітинах біологічного організму. Біологічний вірус перепрограмовує клітину на кшталт того, як це робить комп'ютерний вірус з програмою, на якій він паразитує.

[2] Фото: Автор - http://www.history.org.ua/?l=EHU&verbvar=Gromashevsky_L&abcvar=4&bbcvar=20, Добропорядне використання, https://uk.wikipedia.org/w/index.php?curid=930749

Таблиця 1.3

Термінологія епідемічного процесу	
біологічного	**комп'ютерного**
Джерело збудника інфекції	
заражений (інфікований) організм людини, тварини або рослини, від якої може піти зараження сприйнятливих людей	заражений (інфікований) комп'ютер в мережі, від якого може піти зараження сприйнятливих комп'ютерів
Механізм передачі збудника інфекції	
спосіб переміщення паразита з хворого організму в здоровий, такий, що забезпечує його існування як біологічного виду	спосіб переміщення вірусу з інфікованого комп'ютера в незаражений, такий, що забезпечує його існування як програмної компоненти
Шлях передачі - певна сукупність і послідовність чинників передачі, за допомогою яких реалізується механізм передачі	
Чинник передачі	
об'єкт довкілля, за допомогою якого збудник переміщається з хворого організму в здоровий	компонент інформаційної інфраструктури, за допомогою якого вірус переміщається з інфікованого комп'ютера в незаражений
Сприйнятливий організм	
сприйнятливість - здатність хазяїна хворіти на захворювання, що викликаються збудниками, які проявляються патологічними реакціями, і у відповідь - захисними специфічними (імунітет) і неспецифічними (резистентність) реакціями	сприйнятливість – здатність комп'ютера бути інфікованим вірусом, що проявляється зниженням або припиненням працездатності, або, у відповідь, специфічними можливостями захисту (імунітет) і неспецифічними можливостями захисту (резистентність)
Імунітет	
специфічна реакція організму на укорінення стороннього біологічного агента	специфічна реакція системного програмного забезпечення на впровадження стороннього програмного агента
Резистентність	
комплекс неспецифічних захисних реакцій організму	комплекс неспецифічних захисних реакцій програмно-апаратної системи

Таблиця 1.4

Періоди епідемічного процесу	
біологічного	**комп'ютерного**
Інкубаційний період	
ознаки захворювання проявляються не відразу після зараження особин популяції, а через певний час. Такий період є прихованим, і може тривати до кількох днів і навіть тижнів. Протягом інкубаційного періоду відбувається розмноження й нагромадження мікробів та їхніх отрут, підвищення реактивності організму до збудника	ознаки зараженння комп'ютерів проявляються не відразу після зараження, а через певний час. Такий період є прихованим, і може тривати від кількох годин до кількох днів, тижнів і навіть довше. Протягом цього періоду може відбуватися розмноження вірусу, але деструктивні дії не відбуваються
Період провісників розповсюдження хвороби (продромальний період)	
характеризується наявністю у певної кількості особин деяких загальних ознак захворювання (підвищення температури, загальне нездужання тощо), а також явних ознак захворювання	характеризується проявом деструктивних дій вірусу на деяких комп'ютерах
Період розпалу епідемії	
епідемічний процес поступово досягає високої інтенсивності, тримається на цьому рівні певний час, в окремих випадках досить тривалий (цей час є неоднаковим при різних захворюваннях)	епідемічний процес майже миттєво досягає високої інтенсивності, тримається на цьому рівні нетривалий час, але рівень заподіяної шкоди може бути досить значним
Період одужання (реконвалесценції)	
при сприятливих умовах хворі особини поступово переходять у стадію одужання. При багатьох інфекційних захворюваннях клінічне одужування не збігається за часом зі звільненням інфікованого організму від збудника хвороби	при запровадженні відповідних антивірусних засобів заражені комп'ютери швидко переходять у стадію відновлення працездатності. При цьому «одужування» збігається за часом зі звільненням інфікованої системи від збудника.

Але мікроби паразитують на клітині, використовуючи її ресурси, отруюють її тощо, але не перепрограмовують. З іншого боку, хоча мікроби не перепрограмовують клітину, але вони перепрограмовують дію організму в цілому. Такі комп'ютерні віруси, що діють в масштабі

всього комп'ютерного «організму», теж існують, і їх чимало. Отже й тут є аналогія комп'ютерних та біологічних збудників епідемій.

Принципова відмінність може бути у меті. Біологічні віруси мають на меті вижити за рахунок паразитування на організмі хазяїна. Комп'ютерні віруси можуть діяти не задля власного виживання, а задля цілей, які їм задає зовнішній «хазяїн» і яких вони будуть добиватись будь-якою ціною.

Іншою відмінністю є об'єкт атаки. В біологічному світі таким об'єктом є сам біологічний організм, а в комп'ютерному це не є обов'язковим. Метою комп'ютерної атаки можуть бути і програмне забезпечення комп'ютера, й інформація, яка зберігається в комп'ютері, і отримання доступу до інших комп'ютерів та інформаційних ресурсів.

Процедура атаки може бути багатоетапною та включати не тільки цифрові методи, але й методи соціальної інженерії.

В обох випадках використовують аналогічні засоби протидії – вакцинацію. Вакцинація в медиціні — це введення в організм антигенного матеріалу з метою породити імунітет до інфекційної хвороби, який запобігає зараженню або ослабляє його негативні наслідки. В комп'ютерній сфері під вакцинацією розуміється встановлення антивірусних програмних засобів.

Але вакцинація і там, і там працює, якщо певний збудник захворювання є відомим. На жаль, нові збудники постійно з'являються в обох сферах, особливо це стосується комп'ютерної. Загроза, яка є невідомою, має назву загрози «нульового дня» і проти неї певний час не існує запобіжних матеріалів (засобів). В медицині в такому випадку радять виконувати передусім загальні санітарно-гігієнічні правила та вводять режим карантину. Навіть серед відомих захворювань існує така їх множина, яку зараховують до «хвороб брудних рук». Якщо мити руки частіше, носити маску, користуватися індивідуальними засобами гігієни, тоді ймовірність того, що хвороба омине, зростає суттєво. Аналогічно і щодо комп'ютерного світу. Не чіпати будь-що в Інтернеті, активувати антивірус та міжмережний екран (firewall), не під'єднувати флеш-носії до сумнівних комп'ютерів - і цифрові небезпеки також

оминуть з набагато більшою імовірністю. Зазвичай це називається цифровою гігієною. Цифровий карантин реалізується теж просто – від'єднати комп'ютер на певний час від мережі.

З викладеного випливає висновок, що потрібно адаптувати досвід медицини та біології щодо боротьби з інфекціями для подальшого застосування у галузі захисту інформаційних систем [25]. При цьому необхідно враховувати технічні можливості щодо ідентифікації та кластеризації можливих небезпечних зовнішніх об'єктів, які інформаційно взаємодіють з системою, яка захищається [18].

2 Методи та засоби захисту від різних типів вірусів

«Усе, що може зіпсуватися, — псується. Наслідок: усе, що не може зіпсуватися, — псується теж».

Закон Чизхолма

Типи шкідливих програм, що впливають на виконання управлінських функцій. Формування захищеного середовища інформаційного простору органу управління. Антивірусне програмне забезпечення. Управління інформаційною безпекою

2.1. Типи шкідливих програм, що впливають на виконання управлінських функцій

Шкідливі програми впливають на різні сфери діяльності, але найбільш чутливо їх руйнівна дія проявляється саме у сфері управління та прийняття рішень, адже в сучасних умовах широкого використання інформаційних технологій наслідки прийнятих рішень (або неприйнятих) з причин порушення функціонування технологічних засобів можуть бути фатальними, особливо в сфері управління критичними інфраструктурами суспільства.

Процеси управління (менеджменту) та прийняття рішень є визначальними з погляду ефективності діяльності підприємств (організацій, установ) як головних елементів економічної структури

країни. Саме тут важливим є підвищення ефективності роботи управлінського апарату, адже в умовах інформаційного суспільства домінують нові виклики управління, які вимагають ефективно реагувати на запити та пропозиції клієнтів, забезпечувати відкритість діяльності на базі використання нових інформаційних технологій.

Динамічною складовою менеджменту та процесів прийняття рішень в органах управління виступає інформація, а найважливішими складовими цих процесів є інформаційні потоки і ресурси, а також телекомунікації та всесвітня мережа. Завдяки цьому характерною рисою сучасності стали явища суттєвого зростання об'ємів інформації, що обробляється, і масовості інформаційних потоків.

Управлінське рішення — це результат аналізу, прогнозування, економічного обґрунтування та вибору альтернативи з множини варіантів, які спрямовані на досягнення конкретних цілей системи управління.

Специфічною функцією управління є сукупність однотипних операцій, що виконуються працівниками ОУ на різних рівнях управління. Серед них основними операціями є:

- аналіз стану справ в галузі, якою опікується ОУ;
- підготовка та прийняття управлінських рішень;
- видання розпоряджень;
- контроль виконання доручень;
- інструктаж підлеглих;
- аналіз стану справ в апараті ОУ;
- та ін.

При цьому особа, що приймає рішення (ОПР) як основний елемент системи управління знаходиться під впливом низки чинників, які в основному мають інформаційну природу (рис. 2.1).

Отже, можна зробити висновок, що ОУ є складною соціальною системою, яка пов'язана специфічними відносинами з багатьма об'єктами зовнішнього середовища. Нарешті, ОУ є інформаційною системою у широкому розумінні, основним типом діяльності якої є

збирання та опрацювання інформації, генерування нової інформації, нового знання, що перш за все відбивається на підготовці рішень.

Основним носієм інформації в ОУ є документ, а процеси ведення і опрацювання документів отримали назву діловодства (справочинство).

Реальні ситуації, що вимагають рішення, потребують опрацювання значного об'єму інформації та зазвичай є суттєво суб'єктивними. Тому теоретичні дослідження і практичний досвід в адміністративному управлінні на цей час спрямовані на скорочення часу прийняття рішень, зниження суб'єктивності процесу прийняття рішення, збільшення його науковості.

Рис. 2.1. Система управління як інформаційна система

Водночас відкритість діяльності як новий сучасний виклик управління потребує забезпечення реалізації трьох складових:

- ведення інформації про діяльність підприємства (організації, установи);
- існування механізму, який би в автоматизованому режимі надавав інформацію громадськості;

• налагодження системи автоматизації відповідей ОУ на запитання й запити громадян (клієнтів).

Виходячи з викладеного вище, можна зробити висновок про те, що при реалізації цілей управління в сучасних умовах ОУ мають вирішувати комплекс задач управління та забезпечення взаємодії з суспільством, використовуючи певні засоби автоматизації та присутності у веб-просторі.

Саме наявність в інфраструктурі ОУ мережевої складової суттєво підвищує рівень небезпеки стосовно зараження зловмисними програмами. Поширення вірусів, впритул до епідемічного напряму, залежить від складності мережі. На сьогодні існує наступна класифікація мереж, в яких поширюються віруси.

HM (Homogenous) – гомогенна мережа, тобто однорідна за своїм складом. В такій мережі кожен об'єкт має можливість з'єднання з будь-яким іншим об'єктом напряму. Такі мережі також є однорівневими.

SF (Scale Free) - безмасштабна мережа, масштабно-інваріантна мережа, якій відповідає граф, в якому ступені вершин розподілені за ступеневим законом. Емпірично встановлено, що чимало з природно виниклих мереж гарно моделюються безмасштабними мережами, як-то: соціальні мережі (зокрема мережі співпраці, наприклад акторів у фільмах або співавторство математиків у наукових статтях), комп'ютерні (Інтернет), залежності програмного забезпечення, деякі фінансові мережі (міжбанківська платіжна мережа), семантичні мережі, авіалінії, комунікаційні, біологічні (зокрема мережі взаємодії протеїн-протеїн), графи цитувань, посилань в Інтернеті тощо [91].

Необхідно відмітити, що у разі відсутності фільтрації (цензури, вірусного контролю) контенту у вузлах верхніх рівнів, безмасштабна мережа також забезпечує можливість з'єднання кожного об'єкту з будь-яким іншим об'єктом, що, у свою чергу, відповідає умовам функціонування гомогенної мережі. Умова наявності вірусного контролю може бути не виконаною у випадку появи принципово нового виду шкідливого коду зловмисного або ненавмисного призначення, який існуючі системи контролю не помічають. Таким чином, та сама

мережа може бути безмасштабною для відомих типів шкідливого коду та одночасно гетерогенною для невідомих. Крім того, зауважимо, що такі мережі природно є багаторівневими.

ML (Multi Layer) – багатошарові мережі, можуть бути представлені через формалізм безмасштабних SF-мереж, але мають принципову функціональну особливість. У ML-мережі один об'єкт може належати двом або більше різним мережам, що створює певні несподівані ефекти щодо контролю розповсюдження шкідливого коду [105].

Що стосується інформатизації безпосередньо апарату органів управління, то на цей час в них переважно діють спеціалізовані функціональні системи (наприклад, бухгалтерські, фінансового планування, управління постачанням та ін.). Водночас переважна частина робочих місць службовців зв'язана локальною мережею, а також вони оснащені офісними застосуваннями для підготовки та опрацювання документів (рис. 2.2). Вичерпна інформаційна підтримка рішень, а також забезпечення регламентованої бюрократичної роботи на базі визначених процедур і дисциплін формують основне завдання ОУ, яке значною мірою реалізується системою електронного документообігу.

Але прийняття управлінських рішень не відбувається у вакуумі. Рішення приймаються у складному оточенні під впливом різного роду перешкод і обмежень. Одна з головних проблем, яка при цьому виникає, – це забезпечення кібербезпеки інформаційних ресурсів, адже вони знаходяться під постійною увагою злочинців і шахраїв (рис. 2.3). А наслідки перерв та неможливості виконання управлінських функцій часто є непередбачуваними, особливо у надзвичайних ситуаціях та в критичних сферах.

Виходячи з викладеного та враховуючи об'єкти атак основних типів комп'ютерних вірусів можна зробити висновок про найбільш уразливу для них частину управлінської діяльності – документи, підготовлені автоматизованими засобами, зокрема у застосуваннях найбільш поширеного офісного пакету Microsoft Office, а також

повідомлення і документи, отримані електронною поштою (рис. 2.4). Крім того, суттєво уразливою частиною інформаційної інфраструктури є веб-ресурси. На вказані об'єкти в основному націлені макровіруси і хробаки.

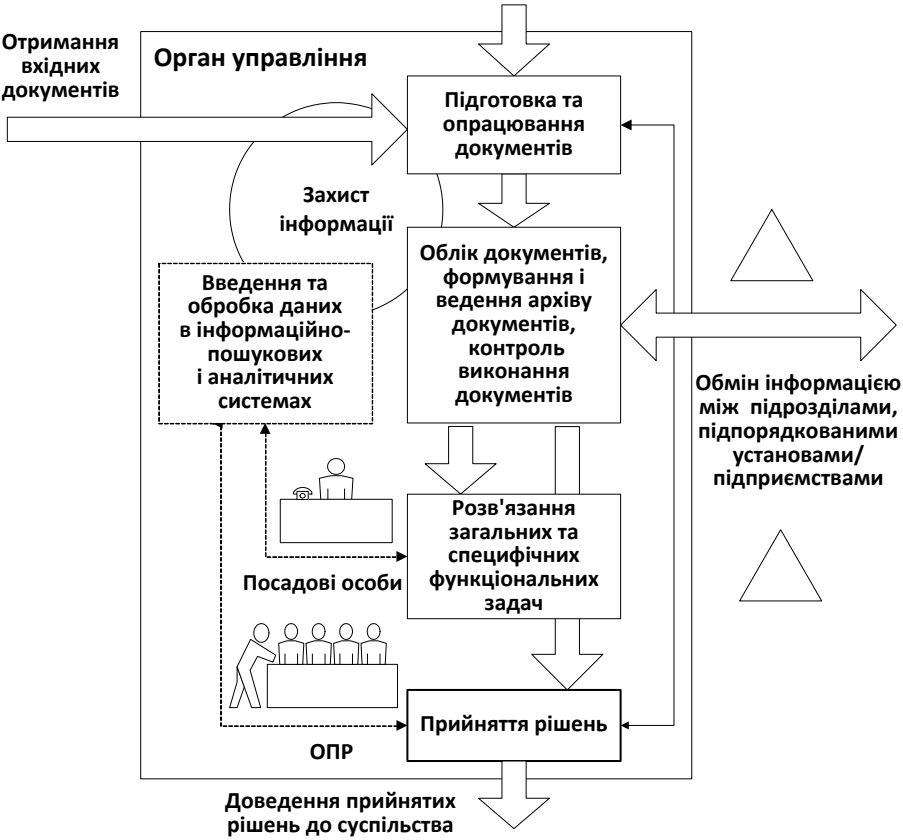


Рис. 2.2. Документальні чинники виконання управлінських функцій

Ситуація ускладнюється тим, що актуальним завданням для органів державного управління є створення публічних інформаційних ресурсів, до яких організовується доступ користувачів через Інтернет.

Такі ресурси використовуються не лише для пошуку й надання інформації, але й для організації та контролю управлінських процесів і функцій, для підтримки прийняття рішень адміністративного управління.

Рис. 2.3. Чинники виконання управлінських функцій в сучасних умовах

На цьому тлі залишається занадто повільним виявлення інцидентів. На форумі Cisco 8 жовтня 2015 р. в Києві старший віце-президент компанії і директор з питань інформаційної безпеки Джон Стюарт повідомів, що середній час виявлення інциденту в галузі IT складає 200 днів, і компанія лише планує досягти його зменшення до 2 днів [28]. Особливе занепокоєння викликає той факт, що близько 70% атак залишаються невиявленими [69, 99]. І, як наслідок, кількість видів атак завжди перевищує кількість технологій захисту, що постійно зростає.

Чим більше є інформації про атаку та її подальший розвиток, тим краще працює кіберзахист. Але зазвичай можливості спостереження

обмежені. Крім того, на спостереження є дуже мало часу через те, що більшість масованих атак доводить систему до епідемічного рівня (рівня непрацездатності) за лічені хвилини.

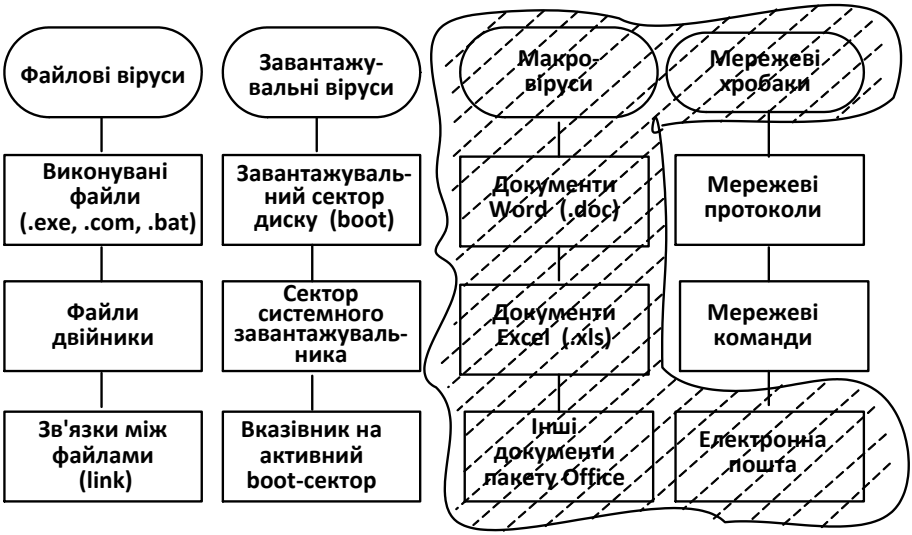


Рис. 2.4. Об’єкти існування вірусів, що найбільш впливають на виконання управлінських функцій (заштрихована зона)

Найнебезпечнішими є атаки нульового дня. Вразливість нульового дня (Zero-day, або 0day) — вразливість програмного забезпечення, яка ще невідома користувачам чи розробникам програмного забезпечення та проти якої ще не розроблені механізми захисту. Сам термін означає, що у розробників було 0 днів на виправлення дефекту, тобто уразливість або атака стає публічно відомою до моменту випуску виробником ПЗ для виправлення помилок (потенційно уразливі робочі копії програми можуть експлуатуватись без можливості захисту).

На даний момент чимало хакерів фокусують свої зусилля саме на виявленні невідомих вразливостей в програмному забезпеченні. Це обумовлено високою ефективністю використання вразливостей, що, в свою чергу, пов’язано з двома чинниками: високим поширенням

уразливого ПЗ, зокрема прикладного (саме таке програмне забезпечення, як правило, зазнає атак), і наявністю часового проміжку між виявленням уразливості компанією-розробником програмного забезпечення і випуском патчів.

Крім створення шкідливих програм, що використовують вразливості нульового дня в програмному забезпеченні, хакери активно працюють і над створенням програм, які неможливо виявити антивірусними сканерами. Ці шкідливі програми також входять у визначення терміну 0day.

Таким чином, перед власниками інформаційних ресурсів ОУ в сучасних умовах постають суперечливого характеру серйозні проблеми забезпечення захищеного середовища інформаційного простору, що суттєво ускладнюють прийняття рішень щодо формування засобів захисту (рис. 2.5).

Рис. 2.5. Проблеми забезпечення захищеного середовища інформаційного простору органу управління

В таких умовах важливим підходом є комплексність захисту - принцип захисту, що передбачає заходи проти всіх небезпечних видів і засобів несанкціонованого доступу до інформації. При цьому оцінка, а ще важливіше, прогнозування захищеності засобів ведення інформації, що функціонує в ОУ, є надзвичайно актуальними при організації та побудові відповідної системи захисту.

2.2. Формування захищеного середовища інформаційного простору органу управління

До складу середовища інформаційного простору ОУ, який забезпечує функціонування веб-ресурсу, зазвичай входять наступні складові (характеристики яких впливають на реалізацію політики безпеки та мають бути враховані під час забезпечення захисту інформації): ОС, фізичне середовище, в якому вона перебуває і функціонує, середовище користувачів, інформація, що обробляється, у тому числі й технологія її обробки. Схему типового інформаційного середовища ОУ наведено на рис. 2.6 [31].

Для визначення можливості застосування тих чи інших контрзаходів необхідно побудувати модель вірусних загроз та здійснити їх аналіз з метою визначення початкового стану захищеності середовища та, відповідно, можливої величини (рівня) шкоди від реалізації загроз. Порядок здійснення цього аналізу може складатись з наступних етапів.

1. Аналіз можливостей ухилення від загроз – ґрунтується на розумінні того, що таке ухилення є припустимим. Це може бути запобігання, або зведення до мінімуму підключення робочих станцій, що є елементами середовища, до інших мереж, наприклад до Інтернету; обмеження повноважень користувачів до мінімально допустимих, коли забезпечується реалізація лише основних функцій.

2. Аналіз можливостей зміни характеру ймовірного ризику – ґрунтується на розумінні того, що така зміна може бути застосованою, якщо неможливо іншим шляхом запобігти ймовірним загрозам, або зменшити можливу шкоду. Заходами такого підходу можуть бути включення до договорів з постачальниками прикладних програмних засобів, загальносистемного програмного забезпечення та інших програмних компонентів, умов щодо відшкодування збитків, які виникли через використання цих засобів шкідливими програмами.

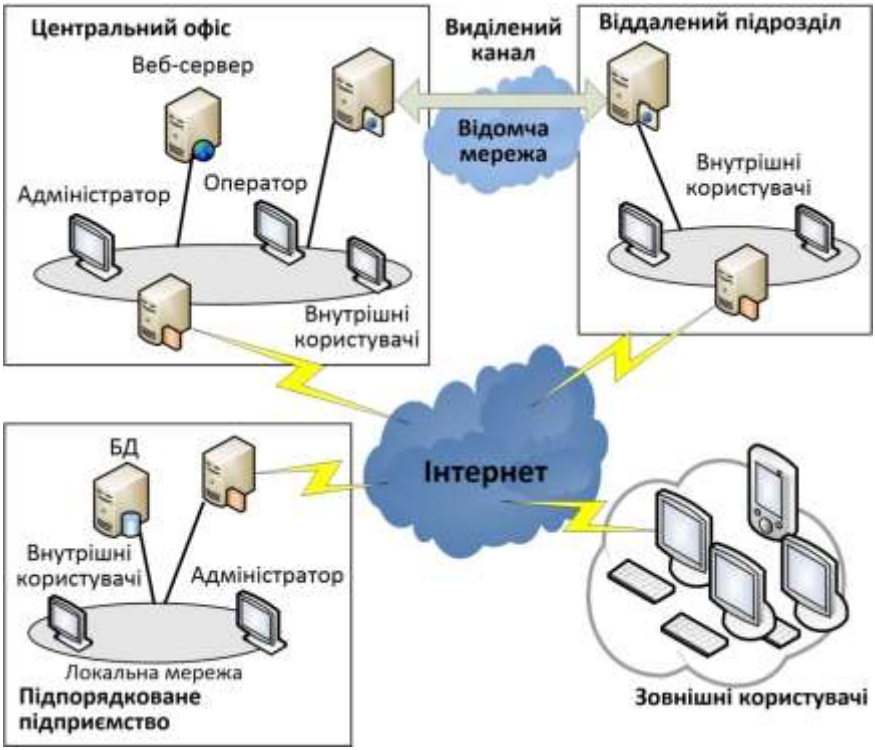


Рис. 2.6. Схема типового інформаційного середовища органу управління

3. Аналіз можливостей сприйняття допустимості реалізації певних загроз з певним рівнем залишкового ризику і, відповідно, певним рівнем збитків – ґрунтується на розумінні того, що деякі з ризиків мають низьку ймовірність та низький рівень шкоди, або не можуть бути зменшеними до мізерно малої величини. На практиці, навіть після вжиття певних контрзаходів, перелік ризиків, хоч і зменшується, але залишається ще значним. Для таких загроз необхідно або знати, або визначити величину залишкового ризику та рівень витрат на його зменшення.

4. У разі неприйнятності деяких із підходів визначеного порядку управління ризиками, для подальшого зменшення можливості реалізації

загроз необхідно застосовувати заходи та засоби захисту. Зрозуміло, що відтепер розмову слід вести про захист лише від тих загроз, від яких не можна ухилитися, змінити їх характер чи сприйняти допустимість їх реалізації з певним рівнем залишкового ризику і, відповідно, певним рівнем збитків. На цьому етапі важливим є застосування прогностичного моделювання реалізації таких загроз для остаточного визначення ризиків і можливих збитків.

Загалом комплекс засобів захисту складається з компонент, наведених на рис. 2.7 [5].

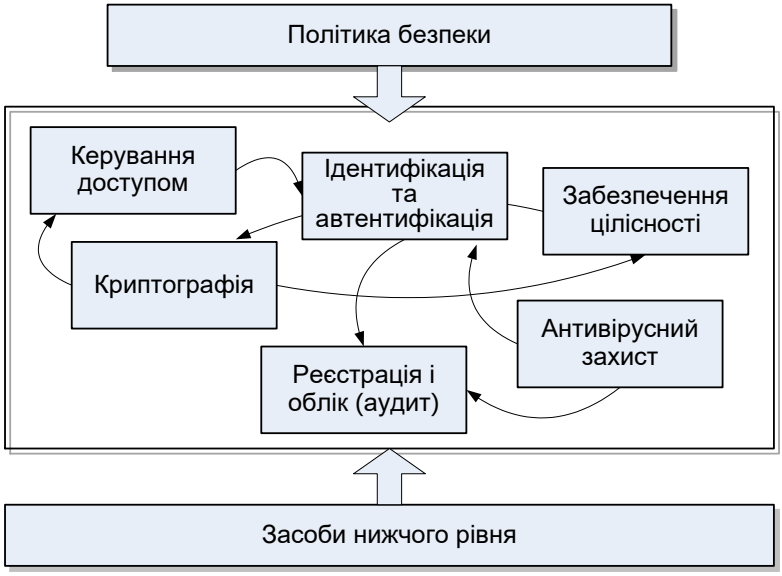


Рис. 2.7. Типовий комплекс засобів захисту автоматизованої системи

Архітектура вказаних засобів зазвичай будується за рівнями, і найвищим рівнем є політика безпеки. Засоби, розподілені по рівнях структури, взаємодіють один з одним з метою забезпечення окремої задачі захисту, кожна з яких спрямована на запобігання проникненню шкідливих програм.

Ще одним підходом, що дозволяє знизити ризик зараження, є застосування вільного/відкритого програмного забезпечення, яке, по-перше, менш вразливе щодо шкідливих програм, а, по-друге, його архітектура менш приваблива для зловмисників, завдяки меншій поширеності, порівняно з пропрієтарним ПЗ [12, 34, 40].

Але у разі реалізації вірусної атаки найпоширенішим засобом нейтралізації вірусів є програмні антивіруси.

2.3. Антивірусне програмне забезпечення

2.3.1. Загальні відомості

Антивірус є програмою, створеною для захисту від вірусів, виявлення заражених програмних модулів і системних областей, а також для відновлення вихідного стану заражених об'єктів. Антивірус може просто виявляти вірус, або виявляти й видаляти його. Якщо вірус видалити не вдається, тоді заражена програма знищується.

Антивірусне програмне забезпечення (АВПЗ) зазвичай використовує два основних методи для виконання своїх задач:

- перегляд (сканування) файлів для пошуку відомих вірусів, що відповідають визначенню в словнику вірусів (фільтрація за репутацією);
- пошук підозрілої поведінки будь-якої з програм, що схожа на поведінку зараженої програми.

Також іноді використовується й метод пошуку вірусів за допомогою емуляції.

Технології двох основних методів пошуку шкідливого коду представлені на загальній схемі, наведеній на рис. 2.8.

Метод відповідності визначення вірусів в словнику полягає у тому, що антивірусна програма під час перегляду файлу звертається до словника з відомими вірусами.

Рис. 2.8. Загальна схема технології пошуку шкідливого коду

У випадку відповідності якоїсь ділянки коду програми, що проглядається, відомому коду (сигнатурі) вірусу в словнику, програма може виконувати одну з наступних дій:

- вилучити інфікований файл;
- відправити файл в карантин (тобто зробити його недоступним для виконання з метою недопущення подальшого поширення вірусу);
- намагатися відтворити файл, видаливши сам вірус з тіла файлу.

Антивіруси, що використовують метод пошуку підозрілої поведінки програм не намагаються ідентифікувати відомі віруси, замість цього вони відстежують поведінку всіх програм. Наприклад, якщо програма намагається записати якісь дані у файл, що виконується (exe-файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити. Однак цей метод має значну кількість помилкових попереджень.

За методом пошуку, використовуючи емуляцію, програми-антивіруси намагаються імітувати початок виконання коду кожної нової програми, що викликається для виконання, перед тим як передати їй керування. Якщо програма використовує код, що змінюється самостійно, або проявляє себе як вірус (тобто починає шукати інші exe-файли, наприклад), така програма буде вважатися шкідливою. Цей метод також має суттєву кількість помилкових попереджень.

Модель технологій пошуку шкідливого коду складається з двох компонент – технічної й аналітичної. Основні методи цих компонент показані на рис. 2.9.

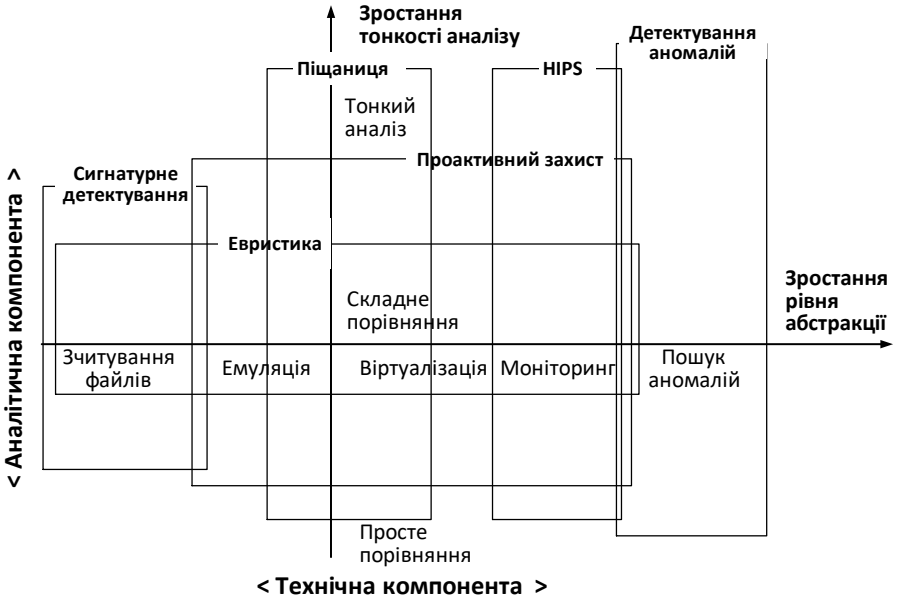


Рис. 2.9. Основні компоненти технологій пошуку шкідливого коду

Технічна компонента — це сукупність програмних функцій і алгоритмів, що забезпечують аналітичну компоненту даними для аналізу. У якості таких можуть виступати, приміром, байтовий код файлу, текстові рядки усередині файлу, одинична дія програми в рамках операційної системи або цілий ланцюжок таких дій.

Аналітична компонента — це система прийняття рішення. Це алгоритм, що аналізує наявні в його розпорядженні дані й виносить про них якесь судження. Відповідно до цього судження антивірус (або інше захисне ПЗ) застосовує встановлені його політикою безпеки дії:

сповіщає користувача, запитує в нього щодо подальших вказівок, поміщає файл у карантин, блокує несанкціоновану дію програми тощо.

Аналітична компонента «приймає рішення» на основі таких методів аналізу:

- просте порівняння – вердикт виноситься за результатами порівняння одного об'єкта з наявним зразком;
- складне порівняння – вердикт виноситься за результатами порівняння одного або декількох об'єктів з відповідними зразками;
- застосування експертної системи – вердикт виноситься в результаті тонкого (інтелектуального) аналізу даних.

Терміни, що використані в наведеній моделі технології пошуку, мають таке тлумачення:

«сигнатурне детектування» – з технічної сторони мається на увазі робота з байтовим кодом файлів, з аналітичної – примітивний спосіб обробки даних простим порівнянням;

«емуляція», або «піщаниця» – аналітична компонента такої технології може бути представлена алгоритмом будь-якого ступеня складності, від простого порівняння до експертної системи;

«евристика» – сукупність дослідницьких методів, що сприяють виявленню раніше невідомого («нечіткий» спосіб розв'язання нечітко поставленої задачі);

«детектування аномалій», «поведінкове детектування», «проактивне детектування» – цими термінами може позначатись широкий спектр технологій – від евристики до моніторингу системних подій;

HIPS (Host Intrusion Prevention System, система запобігання вторгненням) – захист, технічно заснований на моніторингу системних подій. HIPS є засобом проактивного захисту, тобто не містить бази даних сигнатур вірусів і не здійснює їх детектування.

Ефективність технічної компоненти оцінюється за такими показниками:

- навантаження на систему – частка процесорного часу й оперативної пам'яті, безупинно або періодично задіяних у забезпеченні захисту, що обмежує швидкодію системи;
- безпека - мається на увазі ступінь ризику, якому піддається система й дані користувача в процесі ідентифікації потенційно шкідливого коду;
- захищеність - цей параметр відображує уразливість технології, те, наскільки шкідливий код може ускладнити процес власної ідентифікації.

Аналіз цих показників свідчить, що у середньому, чим більш загальним є захист, тим менше він впливає на роботу системи, але й тим простіше його обійти.

2.3.2. Типи програмних антивірусів

Існує чимало типів програмних антивірусів: детектори, фаги, вакцини, щеплення, ревізори, монітори.

Детектори забезпечують виявлення вірусів шляхом перегляду файлів, що виконуються, і пошуку сигнатур. Антивірус, що забезпечує можливість пошуку різних сигнатур, називають полідетектором.

Фаги виконують функції детектора і, крім того, "лікують" інфіковані програми шляхом "викушування" (або, як ще кажуть, "поїдання") вірусів з тіла програми. Фаги, що здатні нейтралізувати різні віруси, називаються поліфагами. Антивіруси-поліфаги ефективні в боротьбі з уже відомими вірусами, тобто такими, чиї методи поведінки вже знайомі розробникам і є в базі програми. Якщо вірус невідомий, тоді він залишиться непоміченим. Головне в боротьбі з вірусами — якомога частіше оновлювати версії програми і вірусні бази.

Вакцини, на відміну від детекторів та фагів, за принципом дії нагадують віруси. Вакцина імплантується у програму, яку необхідно захистити, і запам'ятовує низку її структурних і кількісних характеристик. Якщо таку програму інфікує вірус, тоді при першому ж запуску спочатку керування перейде не до вірусу, а до вакцини, яка

перевірить параметри файлу і виявить код вірусу. І, відповідно, такий файл не буде запускатись.

Щеплення враховує той факт, що більшість вірусів заражає один файл лише один раз (максимально це може відбуватись в два етапи, проте не часто зустрічається) для того, щоб одразу не виявити себе різкою зміною об'ємів файлів. На інфікований файл вірус ставить певну мітку, і більше його не притягує. Отже, програма зі штучною міткою зараження (зі щепленням) зберігає всі свої робочі властивості і є захищеною від вірусу.

Ревізори стежать за станом файлової системи, використовуючи принцип захисту, що застосовано у вакцинах, але характеристики файлів зберігаються ревізором в окремому файлі. Так, для перевірки наступного файлу необхідно наново запускати програму-ревізора.

Монітори – це резидентні програми, що забезпечують перехоплення потенційно небезпечних переривань, які є характерними для вірусів. Монітор запитує в користувачів підтвердження на виконання операцій, наступних після переривання. У випадку заборони чи відсутності підтвердження монітор блокує виконання програми.

Сьогодні шкідливе ПЗ стає все більш спеціалізованим і невловимим, часто його неможливо виявити за допомогою сигнатурних методів. Наприклад, таке ПЗ само собою є інструментом для збору і витягання даних, тому досвідчені хакери використовують різні частини коду для проведення різних етапів своєї хакерської операції, що значно обтяжує визначення такої розширеної атаки.

Тому останнім часом з'явився і успішно розвивається новий антивірусний сегмент, який аналітики назвали STAP — Specialized Threat Analysis and Protection (спеціальні засоби аналізу і захисту). Для продуктів STAP характерне використання більшою мірою не сигнатур, а технологічних методик: пісочниць для попереднього завантаження даних, емуляції, аналізу великих даних, контейнеризації даних.

2.3.3. Орієнтація в середовищі програмних антивірусів

Популярність антивірусних програм значно збільшила світовий ринок цих засобів. Нижче наведено перелік найбільш відомих засобів:

AhnLab V3 Internet Security	eScan Anti-Virus	Kaspersky Anti-Virus
avast! Free Antivirus	ESET NOD32 Antivirus	Microsoft Security Essentials
AVG Anti-Virus	F-Secure Anti-Virus	Panda Cloud Antivirus
AVIRA Antivirus Premium	Fortinet FortiClient Lite	PC Tools Sryware Doctor with AV
BitDefender Anti-virus Plus	G DATA AntiVirus	Qihoo 360 Antivirus
BullGuard Antivirus	GFI Vipre Antivirus	Tencent QQ PC Manager

Одним з методів орієнтації в цьому скопищі програм є відслідковування їх рейтингів, що формуються за результатами тестування найбільш поширених засобів, яке щорічно проводиться відомими дослідницькими компаніями. Зазвичай при тестуванні використовуються дві групи критеріїв – якість захисту й всі інші загальні критерії.

Для оцінки якості захисту враховуються: швидкість реакції, якість сигнатурного детектування, якість евристичного аналізатора, якість поведінкового блокатора, можливість лікування активних заражень, можливість виявлення активних руткітів, самозахист, підтримка пакувальників і кількість помилкових спрацьовувань.

До загальних критеріїв належать: уповільнення роботи системи при використанні антивірусу, зручність інтерфейсу, простота використання, функціональність, стійкість до збоїв, гнучкість настроювань, простота встановлення.

В ході тестування антивірусні рішення випробовуються в найскладніших умовах, зокрема за відсутності оновлення антивірусних

баз і доступу до хмарних сервісів. Таким чином, успіх тестування повністю залежить від технологій проактивного захисту.

Для вишуканих користувачів може бути цікавим тестування ергономічності популярних персональних антивірусів. Для тестування використовується «ідеальний антивірус» із стовідсотковою ергономічністю, під яким розуміється такий продукт, який виконує всі операції за мінімальний час без помилок, який містить всі можливі засоби навчання і реалізує несуперечливу інформаційну модель. З цим еталоном порівнюються результати протестованих антивірусів.

Враховуючи значну довіру користувачів до антивірусних програм, зловмисники навчилися створювати фальшиві антивіруси — програми, які імітують видалення шкідливих програм, або, видаляючи одну шкідливу програму, натомість завантажують іншу.

Практично всі фальшиві антивіруси мають англомовний інтерфейс, їх мішенню в першу чергу є користувачі західних країн. Увесь «бізнес» фальшивок побудований на тому, що користувачі хочуть бути захищеними і готові платити за захист комп'ютера чималі гроші. Для прикладу на рис. 2.10 показана динаміка детектування фальшивих антивірусів в США, Канаді і країнах Західної Європи у 2011-2012 рр. (за даними Kaspersky Lab) [15].

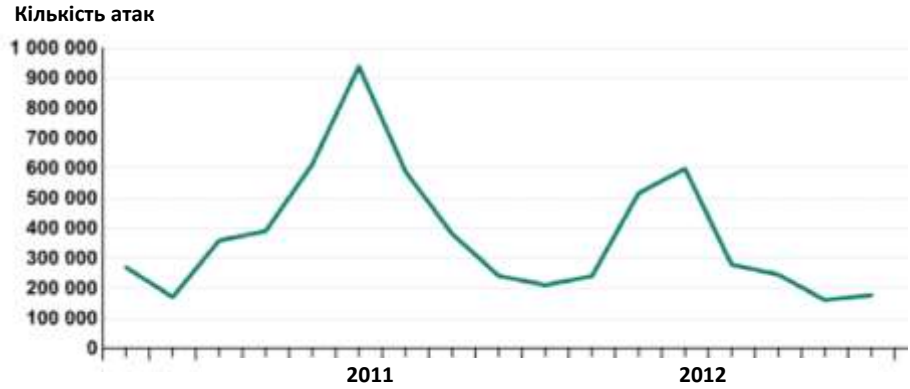


Рис. 2.10. Динаміка детектування атак фальшивих антивірусів в США, Канаді і країнах Західної Європи

Поширення фальшивих антивірусів не стихає. Згідно з повідомленням за квітень 2018 р. (http://vsviti.com.ua/news/82859) співробітники компанії ESET знайшли в магазині Google Play 35 підроблених антивірусів. Фальшиві застосування маскувалися під справжні, однак шахраї копіювали лише оболонку програм. Деякі антивіруси пропонували користувачам оплатити розширену версію, а також використовувати функцію менеджера паролів. Представники Google видалили підроблені застосування з магазину, але до цього фальшиві антивіруси встигло завантажити більше 7 мільйонів людей.

Найпростішою ознакою фальшивого антивірусу є його пропозиція демонстрації можливостей лікування через веб, що є неможливим, адже веб-браузери влаштовані так, що сайт взагалі не має доступу до файлів, які знаходяться на комп'ютері. Іншою типовою ознакою є вимога сплати за користування через SMS – легальні антивіруси віддають перевагу платіжним системам та банківським карткам.

2.3.4. Технології антивірусного захисту

Засоби антивірусного захисту (АВЗ) мають певну функціональну спрямованість (рис. 2.11).

Рис. 2.11. Типи антивірусних комплексів захисту

Водночас найбільш ефективним вважається створення комплексних систем захисту від вірусів, які включають антивірусний захист на всіх рівнях (кінцеві пристрої, мережеві файлові сервери, поштові сервери, інтернет-шлюзи), зі збереженням модульного принципу побудови, а також формування єдиної системи управління та збору інформації про вірусні атаки, відстеження і контроль актуальності баз сигнатур, контроль захищеності кінцевих користувачів, оновлень Windows, налаштувань безпеки завдяки інтеграції з апаратно-програмними рішеннями контролю доступу.

У мережному середовищі (рис. 2.12) сервер антивірусного захисту зазвичай встановлюється перед проксі-сервером, але за брандмауером. Антивірус отримує на вхід той самий потік, який без нього отримував проксі-сервер, виконує перевірку даних, що надходять, на наявність шкідливого коду і передає вже перевірені дані на проксі-сервер. Щоденне оновлення бази вірусних сиґнатур автоматично реалізується через Інтернет за допомогою спеціальних модулів, що забезпечує високий рівень детектування комп'ютерних вірусів.

У мережному середовищі доцільно організовувати централізований керований комплекс антивірусного захисту із забезпеченням взаємодії між його компонентами (рис. 2.13).

Повномасштабного централізованого антивірусного захисту потребують поштові системи (рис. 2.14). Перевірці на наявність вірусів піддаються всі елементи електронного листа – тіло, прикріплені файли (зокрема архівовані та компресовані), вбудовані OLE-об'єкти, повідомлення будь-якого рівня вкладеності. Виявлені підозрілі або інфіковані об'єкти можуть бути вилікувані, видалені або розміщені в заздалегідь визначеній карантинній директорії для подальшого аналізу.

Перед службами захисту інформації та ІТ-підрозділами постійно стоїть завдання аналізу захищеності, тобто перевірки того, наскільки якісно реалізовані або як використовуються механізми захисту інформації, наскільки це відповідає положенням прийнятої на підприємстві політики безпеки. Сервіс аналізу захищеності

призначений для автоматичного виявлення уразливих місць з метою їхньої оперативної ліквідації.

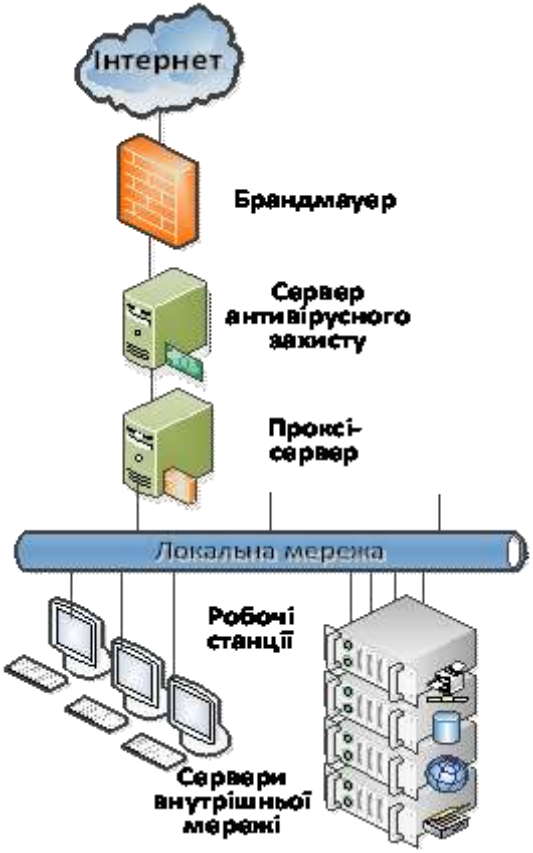


Рис. 2.12. Антивірусний захист в мережному середовищі

Аналіз захищеності є комплексним елементом таких видів робіт (що взаємно перетинаються), як атестація, моніторинг, аудит, а також використання спеціальних автоматизованих засобів виявлення та випередження небажаних вторгнень. Аналіз захищеності допомагає виявити і, як результат, усунути прогалини в захисті до того, як їх зможе використати зловмисник [2].

У першу чергу, маються на увазі не архітектурні (їх ліквідувати складно), а "оперативні" проломи, що з'явилися в результаті помилок адміністрування або через неуважність до відновлення версій програмного забезпечення, як-то: слабкі паролі користувачів, невдало зконфігуровані операційні системи, небезпечні мережні сервіси, невстановлені латки, уразливості в застосуваннях тощо.

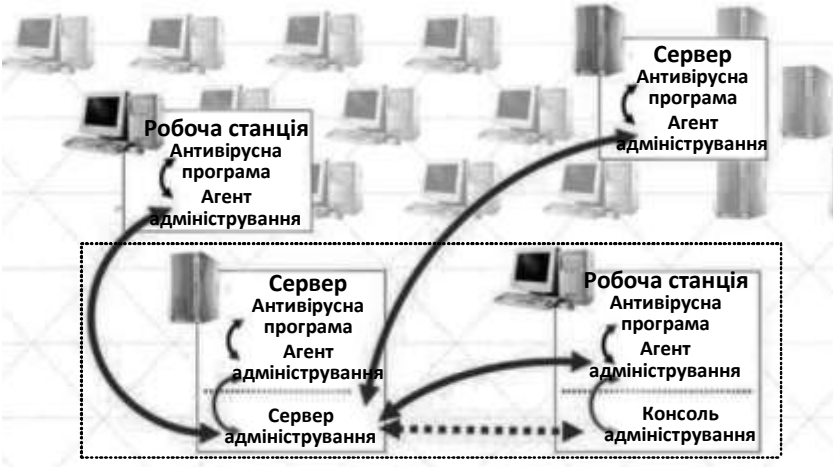


Рис. 2.13. Схема взаємодії компонентів централізованого керованого комплексу антивірусного захисту в мережі

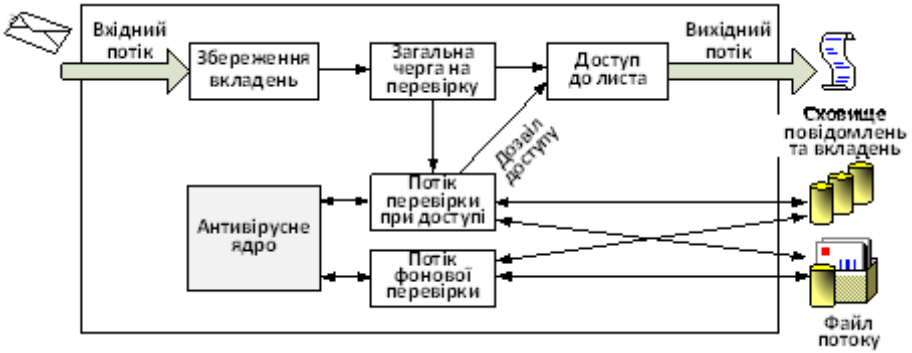


Рис. 2.14. Схема антивірусного захисту для поштових систем

Одним із випереджувальних заходів є проведення огляду АС на предмет виявлення наявності шкідливого ПЗ (зокрема, вірусів). Використовуються різні типи огляду:

- огляд за запитом – вручну перевіряються обрані файли і папки на комп'ютерах;
- огляд у реальному часі (автоматично) – ця функція безупинно перевіряє на наявність відомих вірусів файли, які читаються/записуються, і виконує накопичення статистичних даних (рис. 2.15);
- плановий огляд – перевіряються обрані файли і папки на комп'ютерах АС у запланований час.

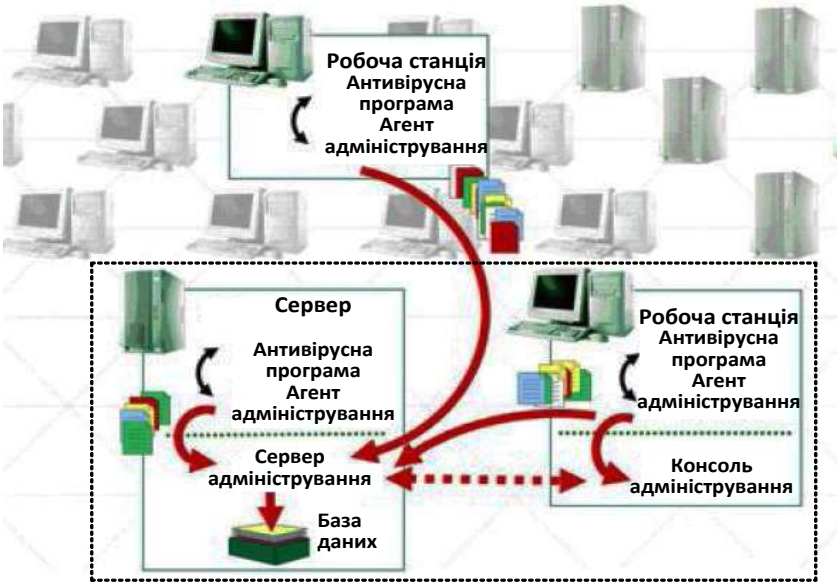


Рис. 2.15. Схема збирання статистики в системі антивірусного захисту

Системи аналізу захищеності, що також мають назву програмне забезпечення для сканування (scanning software) або сканери безпеки (security scanner), як і засоби активного аудиту, засновані на нагромадженні й використанні знань про прогалини в захисті – про те,

як їх шукати, наскільки вони серйозні і як їх усувати (рис. 2.16). Ядром такої системи є база уразливих місць. Найбільш ефективними є мережні сканери (завдяки домінуванню сімейства протоколів TCP/IP), а також антивірусні засоби.

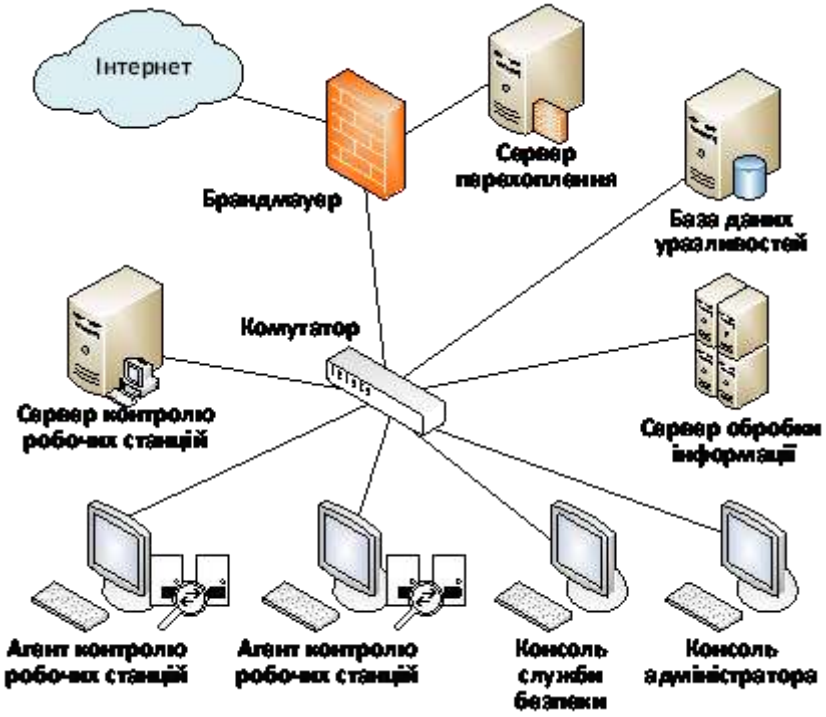


Рис. 2.16. Система аналізу захищеності

Суттєвого значення набуває питання безпеки та захисту в розподілених комп'ютерних середовищах [35, 86]. Найбільш розвинутими і ефективними засобами аналізу захищеності в мережному середовищі є системи виявлення вторгнень IDS (Intrusion Detection System) і системи запобігання вторгненням IPS (Intrusion Prevention System). Комплекс цих систем забезпечує складання "карти" мережі, що містить інформацію про потенційно слабозахищені місця, стан ОС,

роботу застосувань і протоколів, кількість і типи мережевих пристроїв (робоча станція, сервер, маршрутизатор) тощо (рис. 2.17).

Рис. 2.17. Загальна схема IDS/IPS з антивірусною складовою

Маючи вичерпну інформацію про стан мережі в реальному часі, IDS/IPS аналізують лише ті події, які можуть вплинути на безпеку системи, і не обробляють події, які ніяк на ній не позначаться (рис. 2.18).

Рис. 2.18. Схема відбору подій в системі IPS

Крім того, система IDS/IPS полегшує роботу адміністраторів за рахунок того, що може рекомендувати застосовувати ті чи інші правила захисту від загроз, характерних для певного сімейства ОС, які використовуються в організації. Наприклад, якщо співробітник скористається ОС з некоректними параметрами або недозволеним застосуванням, адміністратор зможе дізнатись не лише IP-адресу цього вузла, але й контактні дані користувача.

2.3.5. Аналіз можливостей використання досвіду епідеміології щодо захисту від кібератак

Як було визначено у попередніх розділах, доводиться констатувати, що засоби захисту інформації зазвичай відстають від засобів кібератак. Спочатку виникає новий вид атаки. Після цього приділяється час її вивченню, пошуку способів захисту. Далі витрачається час на реалізацію знайдених способів захисту. І тільки після певного періоду можна говорити про реальний захист від нової атаки. Суперечність полягає в тому, що, з одного боку, для побудови ефективного захисту від нової атаки її необхідно вивчити, а для цього її потрібно зазнати. З іншого боку, якщо вже атака відбулася, то існуючий захист від цієї конкретної атаки може не тільки не встигнути ефективно спрацювати, але й взагалі стати непотрібним - внаслідок знищення інформаційної системи.

Отже, в нульовій точці відліку, у так званий «нульовий день» нових видів атак, інформаційні системи можуть виявитись беззахисними [30]. Тому інформаційні загрози «нульового дня» вважаються найбільш складними.

Подібна ситуація існує і в біологічних системах. Новий вірус (або інфекція) потрапляє в організм, який його ідентифікує лише через певний час. Потім організм знаходить спосіб протидії (захисту). Надалі організм може стати резистентним до такого виду вірусу або інфекції.

Таку схему протидії для інформаційних та біологічних систем можна назвати «сигнатурною». Для надійного захисту потрібна

сигнатура можливої атаки (тобто її характерні ознаки) та заздалегідь розроблені засоби протидії.

Але в медицині відомі й способи безсигнатурного захисту. Наприклад, способи захисту від, так званих, хвороб «брудних рук». Байдуже, яка саме хвороба намагалася попасти в організм з брудних рук, якщо ці руки регулярно мити. Це реалізація так званого випереджувального бар'єрного механізму.

Досвід медицини також надає ефективні способи протидії дуже небезпечним хворобам.

Загальновідомо, що збудник туберкульозу є дуже поширеним в навколишньому середовищі. Більше того, він присутній в організмі у більшості людей. Але активний розвиток цієї хвороби відбувається переважно в послаблених організмах (знижений імунітет, знижений загальний тонус, слабкість внаслідок інших інфекцій, навіть сильне психологічне пригнічення). Цим обґрунтовується порада лікарів – підвищувати загальний тонус організму.

Аналогію можна застосувати і до інформаційних систем. Окремими ознаками високого тонусу інформаційних систем є:

- наявність чітких правил роботи в організації, в її інформаційній системі;
- наявність чітких інструкцій щодо забезпечення інформаційної безпеки;
- наявність чіткої системи реагування на інциденти інформаційної безпеки;
- наявність працівників, відповідальних за інформаційну безпеку, які не розділяють цю функцію з іншими. Наприклад, небажано покладати функцію захисту інформації лише на системних адміністраторів або призначати їх в цій справі головними відповідальними;
- регулярне оновлення захисного програмного забезпечення;
- чітке керування ролями та повноваженнями користувачів;

- інтеграція та взаємодія служби інформаційної безпеки та інших служб захисту організації (зокрема інженерно-фізичного захисту);
- охоплення всього кола питань щодо інформаційної безпеки. Небажано відокремлювати питання кібербезпеки від інформаційної безпеки в цілому.
- регулярне підвищення рівня кваліфікації персоналу з питань інформаційної безпеки (не тільки служб інформаційної безпеки);
- постійне утримання в полі зору нетехнічних засобів порушення інформаційної безпеки (наприклад, методами соціальної інженерії).

Всі ці та багато інших факторів можуть бути складовими загального «позитивного тонусу інформаційної системи», якщо говорити медичною мовою.

Інший медичний спосіб запобігання розповсюдженню нових та відомих хвороб – це карантин, який використовується в разі виявлення відомої небезпечної хвороби або невідомої хвороби.

Також карантин застосовується в разі виявлення біологічних об'єктів, джерело яких ще не було перевірене. Цей варіант є економічно та в часовому сенсі досить витратним. Тому репрезентативною ознакою для прийняття рішення щодо карантину є виявлення факту захворювання. А потім вже під час карантину можна ідентифікувати збудник та шукати засоби ефективної протидії.

2.3.6. Поради і рекомендації з антивірусного захисту

Якими б ефективними не були технології захисту від вірусів, в цій сфері важливе значення мають поради та рекомендацій щодо загального захисту комп'ютера, які напрацьовані відомими розробниками антивірусного захисту. Нижче наведений досвід від компанії ESET [63].

1. Працювати на комп'ютері потрібно під обліковим записом з обмеженими правами. Це є дуже важливою умовою безпечної роботи,

оскільки значно обмежує можливості запущеного шкідливого коду і при цьому не обмежує користувача у роботі зі стандартним колом задач. Права адміністратора необхідні тільки для налаштування операційної системи, інсталяції програмного забезпечення та інших адміністративних задач.

2. Потребує значної уваги робота з електронною поштою. Якщо відправник поштового повідомлення є невідомим, відкривати вкладення з такого листа категорично не рекомендується, що б не вміщувало дане повідомлення, особливо якщо вкладення має розширення .exe або .js. Треба пам'ятати, що банки та інші організації ніколи не пропонують відправити онлайн номер рахунку, PIN-код та іншу конфіденційну інформацію. Ніякі оновлення, патчі, апдейти для комп'ютерів не розповсюджуються поштою. Більше того, навіть якщо відправник відомий, це не гарантія того, що вкладення є безпечним. У таких випадках рекомендується спочатку зберігати вкладення у спеціально створеній папці на жорсткому диску та перевіряти їх антивірусом. Після успішної перевірки вкладення антивірусною програмою відкривайте його вже з цієї папки.

3. Джерелом поширення різноманітних загроз на сьогодні є широко розповсюджені мобільні застосування, які надають можливість користувачам обмінюватися різноманітними повідомленнями. Рекомендується не відкривати підозрілі файли або посилання, отримані від незнайомих авторів, або не з'ясувавши у відправника походження вкладення, не відповідати на повідомлення від невідомих відправників та не додавати незнайомців до контактів. Небажано відправляти у миттєвих повідомленнях конфіденційну інформацію або особові дані, наприклад, номери кредитних карт, банківські реквізити, паролі або такі особові ідентифікаційні дані, як номер телефону та адреса проживання. Також не варто ділитися нік-іменем та адресою електронної пошти.

4. Особливої обережності потребує робота зі змінними носіями (USB-флешки, CD/DVD-диски). Це теж поширений спосіб зараження комп'ютера, як і Інтернет. Небажано користуватись автозапуском з флешок (виринаюче віконце з пропозицією що-небудь завантажити при

підключенні флешки) та відкривати файли зі змінних пристроїв без попередньої перевірки їх антивірусними програмами.

5. Під час використання соціальних мереж потрібно встановити та перевіряти параметри безпеки та конфіденційності, адже при розміщенні даних у соціальних мережах повністю втрачається контроль доступу до інформації. Іншими словами, у випадку необережності можна надати доступ до конфіденційної інформації всьому світові.

6. Не доцільно переходити за випадковими посиланнями. Дуже часто зловмисники користуються довірливістю користувачів, що охоче переходять за посиланням із заманливими назвами і у такий спосіб завантажують та запускають шкідливу програму.

7. Потрібно уникати використання нелегального, «ламаного» програмного забезпечення, оскільки воно може бути шкідливим. Також не слід встановлювати на комп'ютер програмне забезпечення, отримане з неперевірених джерел.

8. Важливою вимогою є забезпечення цілісності даних. Мова йде про те, що результати роботи у вигляді документів, баз даних, поштової бази, будь-яких інших файлів необхідно періодично зберігати в архівах. Потрібно налаштувати систему резервного копіювання важливої інформації, яка в разі інфікування допоможе відновити всі дані. Не рекомендується залишати зовнішній носій для резервного копіювання підключеним до комп'ютера, оскільки це може призвести до втрати копій під час інфікування. Після оновлення ОС Windows слід створювати нові резервні копії.

9. Періодично (приблизно раз на тиждень) потрібно здійснювати повне сканування комп'ютера антивірусною програмою.

10. Рекомендується відключити або обмежити доступ до віддаленого протоколу робочого столу (RDP), а також відключити макроси в Microsoft Office.

11. Нарешті, бажано утриматися, якщо можливо, від використання в закритій (корпоративній) мережі файлів, отриманих з Інтернету.

2.4. Управління інформаційною безпекою

2.4.1. Місце прогнозування в системі управління інформаційною безпекою

Поряд зі стандартними засобами захисту, без яких неможливе нормальне функціонування АС (таких як автентифікація, міжмережні екрани, контроль доступу, системи резервного копіювання, антивірусні засоби), існує необхідність використання систем управління інформаційною безпекою (СУІБ) як основного засобу організації попередження негативних наслідків мережних атак чи інших несанкціонованих дій. Для зниження ризиків необхідно приділяти увагу організації СУІБ АС згідно з державними і міжнародними стандартами, зокрема у відповідності до стандарту ДСТУ ISO/IEC 27001:2015.

Модель управління інформаційною безпекою (управління інформаційною безпекою, information security management) є набором взаємопов'язаних стратегічних і операційних компонентів, що використовуються для створення ефективної системи інформаційної безпеки організації. Кожен компонент, у свою чергу, є набором процесів і практик, які використовуються разом і націлені на один з аспектів безпеки організації.

Серед зазначених компонентів передбачається використання систем моніторингу. Під моніторингом доступу й використання АС розуміється процес виявлення відхилень від реалізації політики управління доступом до інформаційних ресурсів та мережних послуг з метою фіксації неавторизованих дій.

Контроль безпеки мережі (у сенсі захищеності її від шкідливих дій) забезпечується двома методами: аудитом і контролем. Перевіряють ознаки мережної атаки, як правило, за наступними параметрами:

- навантаження на серверне обладнання та його ПЗ (аномально високі рівні завантаження процесора, раптове скорочення вільного місця на дисках, різке збільшення мережного трафіка);

- наявність помилок в журналах і звітах (окремі повідомлення про помилки в лог-файлах програм серверів або журналі подій серверної частини);
- стан потенційно уразливих об'єктів (ненадійне стороннє ПЗ, конфігурація мережі, що змінилася або неперевірена);
- небажані зміни прав доступу до деякого ресурсу або вмісту файлу.

Зазвичай застосовується різне ПЗ моніторингу й контролю АС загалом і мережі зокрема, що здатне як вчасно сповіщати технічних фахівців про виявлену проблему, так і накопичувати статистичні дані про параметри роботи серверів, сервісів і служб, доступних для докладного аналізу. Стосовно результатів їх використання розрізняють помилки першого й другого роду:

- пропуск атак (небажаність їх є очевидною);
- фіктивні тривоги (не менш неприємні, оскільки відволікають адміністратора безпеки від дійсно важливих справ, побічно сприяючи пропуску атак).

Виявлення спроб порушень інформаційної безпеки забезпечується завдяки застосуванню протоколювання і статистичних методів, в яких у найпростішому випадку використовують систему порогів, перевищення яких є підозрілим.

Переваги статистичного підходу полягають в універсальності і обґрунтованості рішень, потенційній здатності виявляти невідомі атаки, тобто у мінімізації кількості помилок першого роду. Мінуси полягають у відносно високій частці помилок другого роду.

Для порівняння – переваги сигнатурного методу: висока продуктивність, мале число помилок другого роду, обґрунтованість рішень. Основний недолік – невміння виявляти невідомі атаки й варіації відомих атак.

Інформація, що збирається системами моніторингу та сучасний розвиток методів моделювання є базою для формування інтелектуальних систем управління інформаційною безпекою (рис. 2.19).

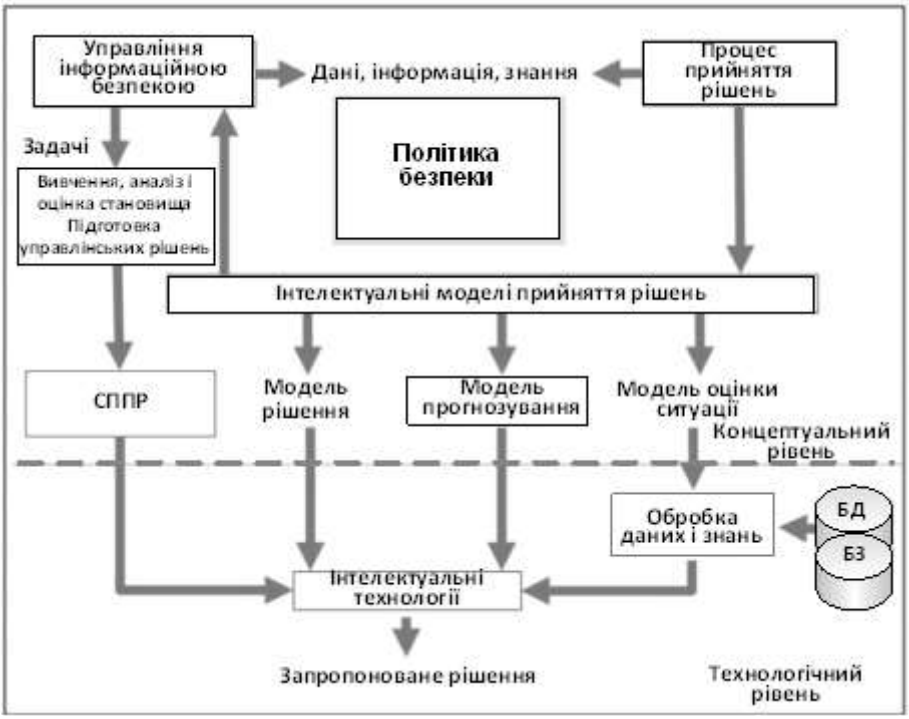


Рис. 2.19. Інтелектуальна система управління інформаційною безпекою

Така система на концептуальному рівні являє собою систему підтримки прийняття рішень (СППР) на основі застосування інтелектуальних моделей прийняття рішень, серед яких центральне місце займають моделі прогнозування.

Оскільки однією з найбільш поширених причин виникнення інцидентів у сфері кібербезпеки є зараження комп'ютерними вірусами, то в науково-прикладному плані проблема прогнозування, тобто передбачення шляхом математичного моделювання інтенсивності розповсюдження вірусного зараження комп'ютерів, які входять до спільного інформаційного простору ОУ та установ, підприємств і організацій, що використовують веб-ресурси ОУ та/або отримують управлінські вказівки та рішення через ці ресурси, стоїть на першому

плані. Іншою проблемою є врахування результатів цього моделювання при формуванні та розвитку захищеного середовища функціонування цього інформаційного простору, особливо в частині захищення веб-ресурсів для запобігання можливості зараження через них комп'ютерів користувачів.

2.4.2. Проблема прогнозування зараження комп'ютерними вірусами

Отже, вкрай важливою задачею є розробка моделі прогнозування розвитку епідемічних процесів зараження комп'ютерними вірусами для того, щоб можна було випереджати основні небезпеки щодо кібератак, прогнозувати розвиток подій та ефективність різних способів захисту.

На основі такої моделі можливе створення системи управління інформаційною безпекою відповідної автоматизованої системи. Використання результатів моделювання дозволяє контролювати розвиток подій як завдяки підбору параметрів захисту, так й за допомогою обрання найбільш адекватних структур системи захисту. Для цього оцінюється ефективність кожного обраного варіанту параметрів і систем захисту.

Оскільки найбільш неконтрольованими є атаки «нульового дня», то їх потрібно якомога скоріше ідентифікувати. Для цього всі об'єкти, що взаємодіють з системою, потрібно розділити на різні групи за ступенем їх небезпеки. Для цього доцільно використати методи кластеризації. Але проблема полягає у виборі параметрів кластеризації (центр кластеризації, радіус кластеризації). У такому разі доцільно з певними модифікаціями використати таксонометричний метод, оскільки він дозволяє автоматично визначити еталон, відносно якого можна порівнювати поведінку всіх об'єктів, що взаємодіють з системою, та, відповідно, розподілити їх за ступенем небезпеки. Найнебезпечнішими при цьому вважаються об'єкти з найбільш

нетиповою поведінкою, тобто об'єкти, які найбільш віддалені від еталону.

Для того щоб теоретичні розробки були практично корисними, доцільно зробити економічні оцінки ситуації та розробити прикладні підходи щодо впровадження розроблених теоретичних положень.

Існує чимало підходів до математичного моделювання комп'ютерних систем, основою яких є теорії зв'язку, масового обслуговування, нейронних мереж, нечіткої логіки та ін. Водночас серед усього розмаїття математичних моделей для опису процесів поширення комп'ютерних вірусів найчастіше застосовуються біологічні підходи моделювання, які протягом значного часу використовуються у галузі медицини. Для прогнозування стану зараження комп'ютерними вірусами об'єктів, що взаємодіють в Інтернеті, можуть бути використані підходи вивчення закономірностей біологічних епідемій.

Організувати протидію епідемії набагато легше, якщо спрогнозувати її розвиток. Передбачення можливих варіантів розвитку епідемій дозволяє вчасно вжити адекватних противоепідемічних заходів, наприклад, для проведення неспецифічної (виявлення та ізоляція захворілих, введення карантину та відміна масових суспільних заходів) та специфічної (вакцинація населення) профілактики грипу [45]. Для правильного передбачення необхідно знати та розуміти внутрішню природу закономірностей розвитку епідемій. Виявлення закономірностей розвитку є корисним як для прийняття рішень щодо протиепідемічних заходів, так і з точки зору збільшення адекватності математичних моделей, які використовуються для прогнозування наслідків епідемії при тих чи інших стратегіях протиепідемічних заходів. Отже, виявлення закономірностей розвитку епідемій на основі аналізу статистичних даних є актуальним питанням. Особливу цінність при цьому становить не лише виявлення математичних закономірностей, але й їх зв`язок із (біологічним, медичним) змістом процесів, що відбуваються [26].

Ці підходи представляють формалізовані методи прогнозування інфекційної захворюваності і розвитку епідемічного процесу, серед

яких: статистичні методи прогнозування (точкові оцінки, регресивні та авторегресійні моделі), методи прогнозування на основі машинного навчання і прецедентів (байєсовські мережі, штучні нейронні мережі, міркування на основі прецедентів), методи прогнозування на базі фільтрації (вейвлет-декомпозиція, експоненціальне згладжування, калмановська фільтрація), математичне моделювання поширення інфекції (аналітичні та імітаційні моделі поширення захворювання), змішані техніки прогнозування [27].

3 ПРОГНОСТИЧНА МОДЕЛЬ ЗАГРОЗ КОМП'ЮТЕРНИХ ВІРУСІВ НА ОСНОВІ КОНЦЕПТУАЛЬНИХ ПІДХОДІВ, ЩО ВИКОРИСТОВУЮТЬСЯ В МЕДИЦИНІ ПРИ ПРОГНОЗУВАННІ РОЗПОВСЮДЖЕННЯ ЗАХВОРЮВАНЬ

«З усіх неприємностей станеться саме та, збиток від якої найбільший.
Залишені без нагляду події мають тенденцію розвиватися від поганого до ще гіршого».

Висновки з законів Мерфі і Чизхолма

Підходи до створення моделей прогнозування загроз нульового дня. Методи прогнозування біологічних епідемій. Використання епідеміологічного підходу до прогнозування інцидентів інформаційної безпеки. Таксонометричний підхід до кластеризації загроз нульового дня. Практична реалізація методу

3.1. Підходи до створення моделей прогнозування загроз нульового дня

3.1.1. Основні складові задачі прогнозування

Якщо розглядати об'єкт моделювання як «чорну скриню», то на її вхід подаються ресурси, а на виході ми отримуємо корисний ефект. Ефект (або корисний ефект) – це те корисне, заради чого й був

започаткований процес, який є об'єктом дослідження. Будь-який результат можна буде вважати корисним ефектом (але інколи з від'ємним знаком). Ефект називають цільовим, якщо він безпосередньо відображує ціль процесу. Ресурс – це те, що процес витрачає задля створення корисного ефекту. Під ресурсами $R = \{m,p,w,x,n,Ef^i,t\}$ розуміємо гроші m, персонал p, обладнання w, матеріальні засоби x, підрозділи n, ефекти діяльності підпорядкованих елементів структур Ef^i, час t тощо.

Для оптимізації управління інформаційною безпекою використовують спеціальні методи теорії оптимального управління, які потребують визначення математичних моделей об'єктів оптимізації, чіткої математичної формалізації цільових функцій та обмежень. Стандартна постановка задачі оптимізації містить детальний опис таких складових, як то модель об'єкту, обмеження, критерій оптимальності.

Модель об'єкту має дозволяти прогнозувати розвиток подій, знаходити оптимальне рішення та прогнозувати наслідки його впровадження. Модель створюється відповідно до певних припущень та має відбивати найбільш суттєве в тій ситуації, в якій знаходиться об'єкт, в умовах прийнятої постановки задачі. Одному і тому самому об'єкту в різних умовах та на різних етапах життєвого циклу можуть відповідати різні моделі.

Розв'язання оптимізаційних задач надає додаткову інформацію про об'єкти, що дозволяє спростити моделі та підвищити їх адекватність. Основні методологічні проблеми оптимізації викликані обмеженістю вхідних ресурсів, вимогою оперативності прийняття рішень, багатокритеріальністю, можливістю зміни цілей, пріоритетів та характеристик об'єктів на наступних етапах планування.

Оптимізаційна процедура має дозволити знайти найкраще рішення в розумінні сформульованого цільового ефекту з урахуванням обмежень на фазові координати та управління. Для розв'язання оптимізаційної задачі необхідним є виконання таких дій [66, 57]:

- визначення мети операції;
- вибір критерію ефективності та визначення обмежень операції;

- розробка математичних моделей критерію якості і обмежень;
- визначення і, у разі потреби, прогнозування вхідної інформації;
- змістовна і формальна (математична) постановка задачі;
- вибір (розробка) математичного апарату для розв'язання задачі;
- аналіз результатів операції згідно з її рішенням і коригування моделей (підвищення їх адекватності).

Після класифікації та спрощення моделей необхідно зробити постановки оптимізаційних задач, відповідно до яких підібрати методи оптимізації.

3.1.2. Вимоги щодо точності моделювання

Для прогнозування можна використовувати попередній досвід [76, 94, 95] або прогнозне моделювання [13, 44]. Попередній досвід не охоплює всіх можливих ситуацій, тому не надає достатньої інформації для прийняття адекватного рішення. Моделювання вимагає адекватних математичних моделей. З одного боку, моделі повинні відображати найголовніші риси процесу, що моделюється. З іншого боку, моделі мають бути достатньо прості для забезпечення їх вхідними даними, для вчасного корегування структури та параметрів моделей відповідно до зміни ситуації або постановки задачі.

Прогнозування кібератак ускладнюється високою невизначеністю факторів впливу. Зазвичай прогноз-модель створюється на основі статистики попередніх атак. Але при загрозі "нульового дня" це неможливо, адже немає статистики. Виходячи з попередньої статистики, можна шукати лише загальні закони, що стосуються "нульового дня" кібератак.

Інший спосіб – визначити фактори впливу, процеси типової атаки та її наслідки. Також потрібно визначитись з рівнем складності моделі. Тут є певні проблеми. Зовсім проста модель буде занадто неточною. Дуже складна модель занадто залежатиме від невизначеності. Складна модель може реагувати на вторинні фактори або мати проблеми із

забезпеченням вхідними даними. Для кожного рівня невизначеності існує рівень оптимальної складності моделі.

Загалом об'єктивним підґрунтям доцільності застосування *грубих моделей* є суперечливі умови використання моделей, а саме: оперативність, точність, наочність, повнота врахування чинників впливу тощо. „Для того щоб система моделей давала опис, який добре відбиває реальність, вона має бути достатньо складною. Але в такому випадку кожен машинний експеримент буде вимагати великих витрат машинного часу. А це значить, що провести велику кількість експериментів – необхідна умова будь-якого аналізу – буває просто неможливо" [43]. „Складність моделей, які належать множині припустимих моделей, обмежена точністю апріорної інформації й інформації, отриманої в результаті експерименту, складністю обчислювальних операцій і (або) технічної реалізації" [46].

Складність моделі має відповідати, з одного боку, складності процесу, а з іншого - можливостям щодо забезпечення вхідними даними. Чим складніша модель, тим складніше забезпечити її вхідними даними, тим вищий ступінь невизначеності, в якій вона функціонує. А з теорії систем відомо, що чим вищий ступінь невизначеності об'єкту, який моделюється, тим простішою має бути його модель [102]. І. Пригожин більш категорично пов'язує необхідність простоти моделей з властивостями самого об'єкту моделювання [42]: «Про „фізичний закон" якого-небудь явища можна говорити лише у тому разі, якщо цей закон є „грубим" відносно граничного переходу від опису з кінцевою точністю до опису нескінченно точного і через це недосяжного для будь-якого спостерігача ким би він не був. Вимога „грубості" за своєю природою не пов'язана зі скінченністю роздільної здатності приладу. Вона відбиває не обмеженість наших можливостей виконувати спостерігання та вимірювання, а внутрішню структуру явищ, які ми описуємо».

Р. Ешбі вважав, що теорію систем можна трактувати як науку про те, як спрощувати системи, які вивчаються [29]. Точність моделі має відповідати точності вхідних даних. Немає сенсу нарощувати точність

підвищенням розмірності моделі при незадовільній точності вхідних даних. За словами А.Н. Крилова, „недостатня точність обчислювань – це помилка. Надлишкова точність – це половина помилки" [29]. Цей висновок підтверджує виведена А.Г. Івахненком залежність квадрату похибок моделі ε^2 від її складності S та шуму $\Theta_1 > \Theta_2 > \Theta_3$ [22].

Розглянемо об'єкт, модель якого створена на основі інформації про поведінку об'єкта впродовж етапу тривалістю ΔT_1. Нехай для його опису з точністю ε необхідно використати S_1 членів поліному Колмогорова-Габора. Тоді опис того самого об'єкту з тією самою точністю на етапі тривалістю ΔT_2 вимагає $S_2 = S_1 \cdot \frac{\Delta T_2}{\Delta T_1}$ членів поліному Колмогорова-Габора, кількість яких є показником складності моделі. При збільшенні тривалості прогнозу T_{pr} пропорційно збільшується кількість вхідних даних, на підставі яких можна забезпечити необхідну точність моделі ε. Квадрат помилки залежить від складності моделі за квадратичним законом [22]. При збільшенні шуму Θ залежність зміщується вверх-ліворуч (рис. 3.1).

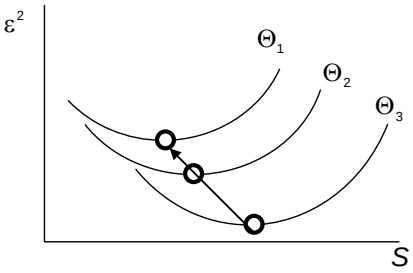
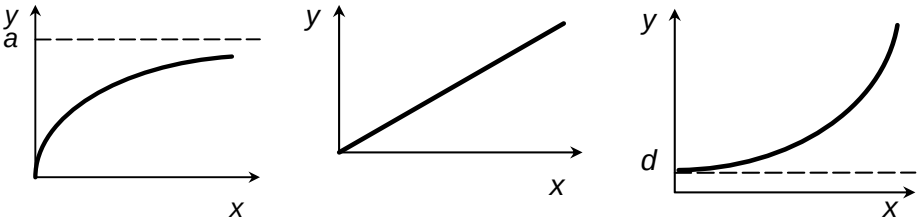


Рис. 3.1. Ілюстрація вимоги спрощення моделей при зростанні невизначеності об'єктів

3.1.3. Базові моделі процесів розвитку

Аналіз існуючих моделей процесів розвитку показав, що найбільш поширеними є лінійні та експоненціальні моделі необмеженого зростання або експоненціального насичення (рис. 3.2), які зазвичай використовуються для процесів розвитку, поведінка яких обумовлена стабільним ресурсним забезпеченням, або які перебувають на одному етапі життєвого циклу.



а) експоненціальне насичення

б) лінійна

в) необмежене експоненціальне зростання

Рис. 3.2. Моделі розвитку

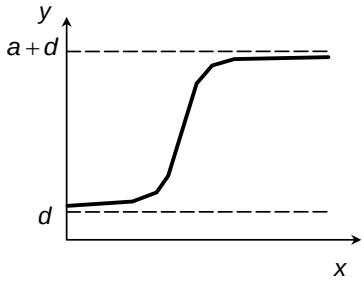


Рис. 3.3. Логістична модель розвитку

Якщо фінансування може варіюватись від нормального до нуля або якщо необхідно розглянути декілька етапів життєвого циклу, то більш адекватною є логістична модель (рис. 3.3) [1], яка містить ділянки, якісно подібні до експоненціальних та лінійних залежностей.

При моделюванні можливі й більш складні якісні картини поведінки процесів розвитку, але вони, здебільшого, складаються з компонент, які досить точно можуть бути апроксимовані лінійними, експоненціальними та логістичними залежностями. Головною перевагою лінійних, експоненціальних та логістичних моделей є їх висока фізична наочність.

Розглянемо основні характеристики названих моделей.

Лінійні моделі. Переваги - простота, наочність, швидкість розрахунків, простота оцінки адекватності, простота підготовки вхідних даних, простота та прозорість облікових даних навіть для нефахівців. Лінійні моделі використовують переважно для добре вивчених об'єктів, які функціонують у суттєво обмеженому діапазоні можливих величин. Поширеним варіантом лінійних моделей ефектів *Ef* є лінійна згортка

$Ef = \sum_{i=1,n} \beta_i \cdot x_i$ оцінок ефектів за окремими елементами x_i з ваговими коефіцієнтами β_i. Велику частку лінійних моделей складають лінеаризовані моделі нелінійних процесів, недоліком яких є вузька зона адекватності. При відхиленні від точки лінеаризації похибка зростає. В окремих випадках лінеаризація навіть призводить до втрати фізичного змісту задачі.

Моделі експоненціального насичення. Експоненціальне зростання з насиченням використане в моделях багатьох об'єктів та процесів, які досягли меж свого розвитку, наприклад, математичне очікування кількості вражених цілей в залежності від вартості системи або заходів [21, 24].

Моделі необмеженого експоненціального зростання. Найбільш відомими є три базових закони розвитку інформаційних технологій [24]: закон Мура (подвоєння обчислювальної продуктивності кожні 1,5 роки), закон Гільдера (щорічне подвоєння пропускної здатності мереж) і „мережевий ефект" Меткальфа (експоненціальне зростання цінності мережі при збільшенні кількості користувачів). Перелічені експоненціальні закони сформульовані з урахуванням постійних змін технології, тобто в припущенні, що обмеження розвитку відсутнє та щоразу при наближенні до обмеження поточна технологія буде замінена більш прогресивною. При відсутності обмежень експоненціальне зростання притаманне різноманітним фізичним процесам (зростання населення, зростання споживання ресурсів [37]).

Логістичні моделі: зростання кількості університетів [41]; збільшення телефонних викликів [17]; результативність рекламної кампанії [1]; виховання в людях фізичних навичок, культури [17].

Процеси росту, в яких логістичні криві послідовно переходять одна в одну: крива загального поступу науково-технічного розвитку [20]. Загальний вигляд залежності, яка узагальнює результати багатьох змін технології, звичайно добре апроксимується експонентою, що відповідає першому основному закону розвитку науки згідно Д. Прайса [41]. Але нагадаємо його другий основний закон розвитку науки:

«... яким би явним не було експоненціальне зростання, воно має наприкінці виявитись логістичним, тобто включати перехідний період кризи, який розташований з обох сторін від середньої точки приблизно на час життя одного покоління».

Необмежене експоненціальне зростання апроксимує послідовність багатьох логістичних складових. Наприклад, на рис. 3.4 товста лінія є експоненціальним трендом світового розвитку, тонка безперервна лінія – розвиток конкурента №1, перервна – розвиток конкурента №2. Припустимо, що на першому етапі (перша логістична функція) рівень розвитку конкурентів збігається. Наприкінці етапу він навіть збігається з експоненціальною залежністю тренду світового розвитку. Здається, що рівень розвитку достатній і не потребує додаткових зусиль. Але після того як логістична крива увійшла в зону насичення та почала наближатися до кривої тренду, треба зрозуміти, що оскільки тривалий час не було змін, то вони мають відбутись найближчим часом. Потрібно інтенсифікувати зусилля щодо розвитку та зміни відповідних інноваційних ресурсів так, як це зробив конкурент №1. Конкурент №2 почав підготовку інновації пізніше і, як результат, отримав менший конкурентний потенціал.

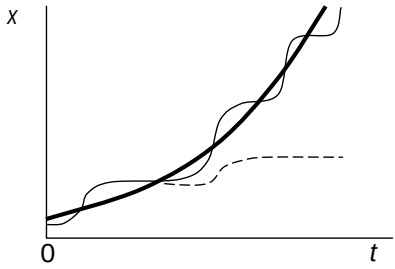


Рис. 3.4. Залежності розвитку як функції часу

Отже, для основи моделей розвитку процесів інформаційної безпеки доцільно обирати логістичні залежності, які поєднують високий ступінь адекватності з невеликими працевтратами на визначення параметрів.

3.2. Методи прогнозування біологічних епідемій

3.2.1. Огляд існуючих підходів щодо моделювань біологічних епідемій

З огляду на важливість проблеми над питанням досліджень моделей епідемій працювало чимало фахівців. В багатьох роботах щодо моделювання епідемій розглянута історія створення моделей епідемій як біологічних [10, 58], так й комп'ютерних [25, 30]. Огляд основних внесків, передусім щодо біологічного моделювання, наведено в табл. 3.1.

3.2.2. Перехід від моделей біологічних епідемій до епідемій комп'ютерних

Питання подоби біологічних та комп'ютерних епідемій вивчались досить давно [60, 61, 73]. Загальним недоліком досліджень того часу є спрощення підходу щодо порівняння. Фактично ці моделі обмежувались моделями типів SI, SIS, SIR. З початку 2000-х років трансфер досвіду моделювання біологічних епідемій в комп'ютерну галузь стала більш цілеспрямованою та системною [15]. Як принципово новий крок щодо моделей кібератак цього періоду найчастіше відзначають роботу [96]. Новий поштовх до розвитку моделей був наданий появою хробака Code Red, який використовував випадкову генерацію IP-адрес вузлів у мережі: 13.06.2001 версія CRv1 [96] та 19.07.2001 версія CRv2 (за 14 годин було інфіковано більше 359 000 комп'ютерів, час подвоєння кількості заражених вузлів 37 хвилин) [80, 81].

На основі емпіричних даних щодо епідемії Code Red була побудована модель RCS (Random Constant Spread), яка дала високий рівень збігу даних щодо прогнозу розвитку епідемії та статистичних даних щодо епідемії CRv1 [96, 92, рис. 1] (рис. 3.5).

Таблиця 3.1

№	Автор	Рік	Сутність підходу
1.	Bernoulli [55]	1760	Вперше застосував найпростіший математичний апарат для оцінки ефективності профілактичних щеплень проти натуральної віспи
2.	Euler [64]	1767	Запропонував рівняння щодо динаміки популяцій
3.	Farr [65]	1840	Вперше отримав математичні моделі показників руху епідеміологічних показників на основі статистичних показників смертності населення Англії (Уельса) від епідемії натуральної віспи в 1837-1839 роках
4.	Lotka [77]	1907	Перевідкрив рівняння Ейлера в дещо модифікованому вигляді: $$B(t) = \int_0^t B(t-a)\,p(a)m(a)dt$$ де B – кількість птахів; t – час; a – вік; p – ймовірність виживання; m – ступінь спроможності надати потомство
5.	Ross [90]	1911	Моделював розповсюдження малярії
6.	Kermack, McKendrick [74]	1927	Одне з перших ретельних досліджень епідеміологічних моделей, зокрема модель SIR часто називають саме їх ім'ям.
7.	Bartlett [54] Kendall [72]	1949 1956	Подальший внесок в розвиток стохастичних моделей [58]
8.	Бароян, Рвачев, Иванников [4]	1977	Найбільш системні моделі, які використовують інтегро-диференціальні рівняння в частинних похідних. Загалом моделі дозволили зробити успішні прогнози щодо початкових періодів епідемій грипу 1971-1972, 1973, 1975 и 1976 років та були перевірені на основі статистики близько 170 епідемій в більш ніж 100 містах СРСР [3, 4, 10, 11]
9.	Боєв [6 - 11, 56]	1991	Суттєво розвинув попередні дослідження щодо загальних підходів до моделювання інфекційних захворювань. Універсальність його моделей була перевірена на задачах прогнозування розвитку раптових внутрішньо-лікарняних інфекцій у немовлят, прогнозування наркотизації молоді, моделювання різних видів грипу, зокрема пташиного, атипової пневмонії, ящуру, віспи, африканської чуми свиней, сказу, ВІЧ-інфекцій, гепатиту, посттравматичних стресових розладів, масової паніки, бойових інфекцій в актах біотероризму.

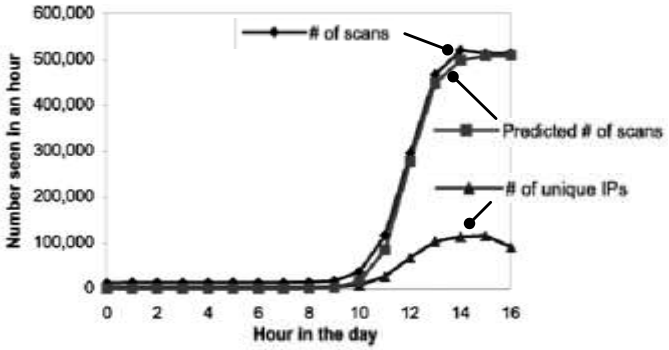


Рис. 3.5. Порівняння прогнозу розвитку епідемії та статистичних даних щодо епідемії CRv1 [80, 81]

Зростання епідемії хробака CRv2 у часі демонструють рис. 3.6 – 3.8 [81]. Експоненційне зростання між 11:00 і 16:30 UTC в логарифмічному масштабі має лінійний вигляд (рис. 3.8).

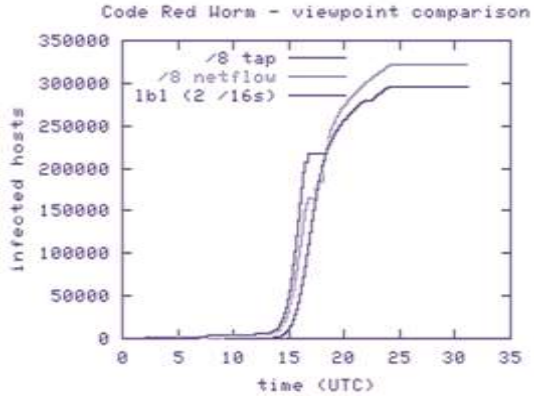


Рис. 3.6. Кількість інфікованих вузлів у часі серед тих, що контролюються в різних мережах (UCSD, LBL) [81]

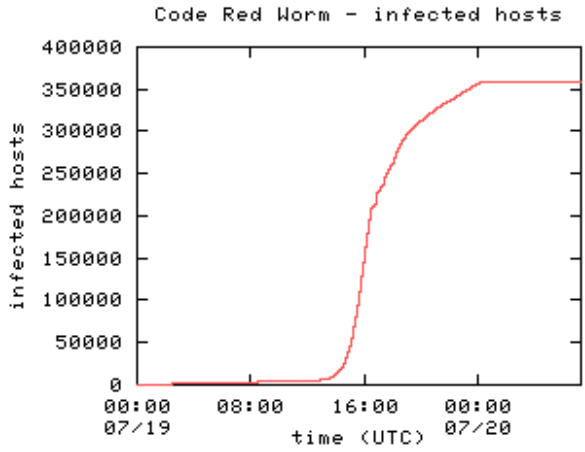


Рис. 3.7. Сумарна кількість заражених вузлів у часі [81]

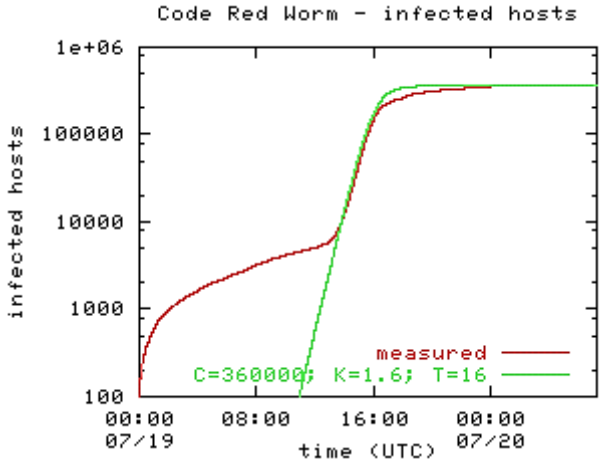


Рис. 3.8. Експоненційне зростання між 11:00 і 16:30 UTC в логарифмічному масштабі [81]

Швидкість розповсюдження має пік в зоні 16:00 (рис. 3.9) [81]. Після початку атаки первісно заражені комп'ютери встановлювали латки для ліквідації вразливостей, перезавантажувались або

фільтрувались, внаслідок чого перестали виконувати задачі хробака щодо пошуку вразливих вузлів (рис. 3.10, 3.11) [80, 81].

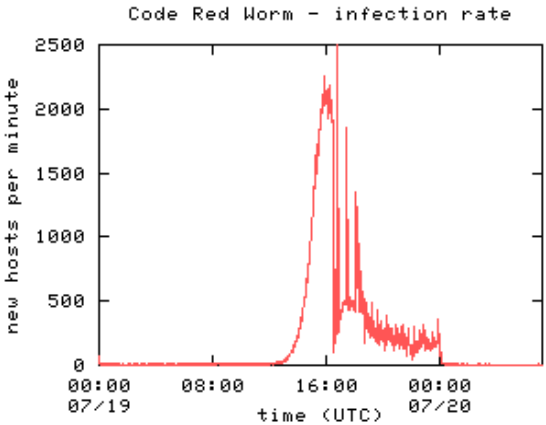


Рис. 3.9. Швидкість поширення хробака (кількість інфікованих вузлів за 1 хвилину) [81]

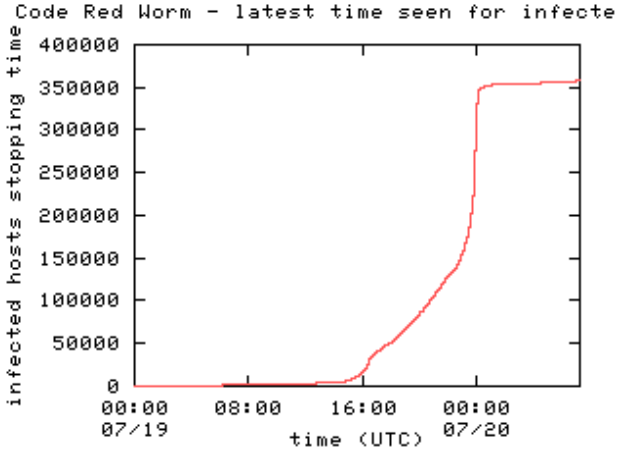


Рис. 3.10. Загальна кількість дезактивованих вузлів у часі [80, 81]

Модель RCS дала також непогану збіжність результатів прогнозу та даних статистики щодо розповсюдження хробака CRv2 (рис. 3.12) [92].

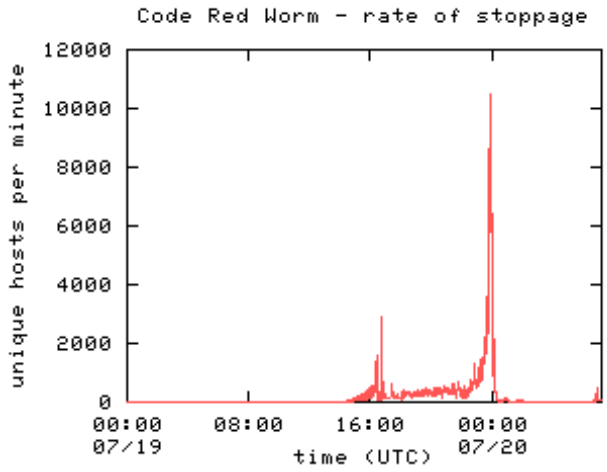


Рис. 3.11. Швидкість дезактивації вузлів у часі [80, 81]

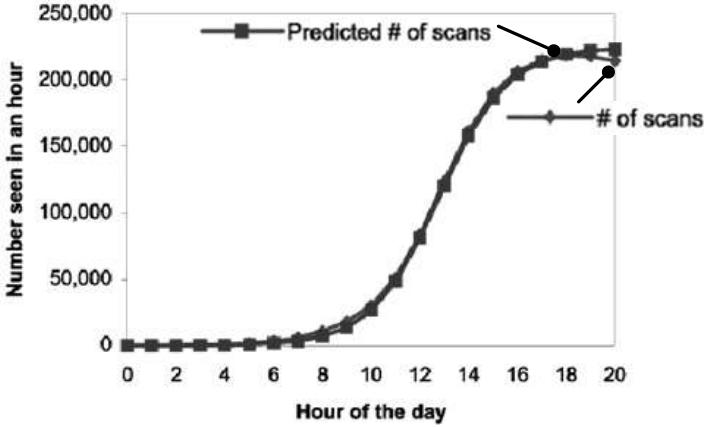


Рис. 3.12. Порівняння прогнозу розвитку епідемії та статистичних даних щодо епідемії CRv2 [92]

Модель RCS дала також гарний збіг прогнозу та статистичних даних для хробака Sapphire Worm (інші назви SQ-Hell або Slammer). Час подвоєння заражених вузлів становив 8,5 секунд (!!!), загальна кількість заражених вузлів 75 000 (рис. 3.13) [92].

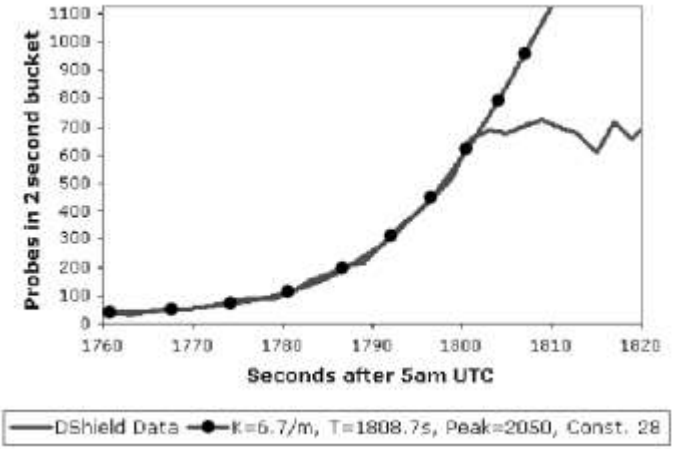


Рис. 3.13. Порівняння прогнозу розвитку епідемії та статистичних даних щодо епідемії Sapphire Worm [92]

Але, як бачимо, прогноз моделі гарно збігається зі статистикою лише у першій частині зараження. Далі мережа виявляється неспроможною обслуговувати таку кількість запитів від Sapphire Worm. Це зайвий раз підштовхує до думки про те, що гарна швидкість мережі потрібна там, де вона дійсно потрібна. В інших випадках її доцільно зменшувати у профілактичних цілях.

Розвиток епідемій має свої закономірності, але інколи одночасно збігається настільки багато різних факторів, що ззовні процес здається хаотичним. Тому при пошуку закономірностей розвитку епідемій необхідний ретельний аналіз статистичних даних одночасно з відокремленням закономірностей вже відомих з інших джерел, зокрема формалізованих у вигляді математичних моделей. При аналізі закономірностей розвитку епідемій можливі дві крайнощі:

1. Суто математичний (статистичний) підхід, в якому виявлені математичні закономірності наявного статистичного матеріалу, що ховають фізичний зміст розвитку епідемій.

2. Змістовний підхід, в якому в спрощеному вигляді виявляються головні чинники розвитку епідемій, а малозначні фактори на даному етапі аналізу не враховуються.

Так, в попередніх дослідженнях [50], виходячи з результатів математичного моделювання, були встановлені такі умови виникнення епідемій:

1. Поява певної кількості хворих або осіб, які знаходяться в стані інкубаційного періоду (внаслідок прибуття означених осіб з інших регіонів або внаслідок формування нового штаму вірусу безпосередньо в регіоні, що розглядається).

2. Певне співвідношення частки несприйнятливих осіб та умов передачі інфекції від хворих до сприйнятливих осіб. Математично це визначається певним співвідношенням коефіцієнту сприйнятливості до зараження K_S та коефіцієнту передачі інфекції K_E.

Достатньою умовою виникнення епідемії є одночасне виникнення першої та другої необхідних умов. Важливе те, що кількість первинно інфікованих для рівня епідемії не має особливого значення. Не має значення 19 чи 20 інфікованих осіб з'явилось в регіоні на початку епідемії. Але різниця в одну особу у випадку 0 або 1 є вирішальною. Тобто малозначні фактори – поняття ситуаційне і вимагає ретельного аналізу всіх можливих взаємозв'язків.

Потрібно проаналізувати фактори, що впливають на розвиток епідемій, а також виявити основні закономірності активації означених факторів та закономірності розвитку епідемій на основі статистичних даних, і пов'язати ці закономірності з відомими математичними моделями епідемій з метою визначення шляхів подальшого вдосконалення останніх.

З цією метою розглянуто динаміку епідемій грипу в Україні за статистичними даними Міністерства охорони здоровя України з 2003 до 2010 року [39]. Такий віддалений у часі період обраний для того, щоб уникнути можливого викривлення інформації посадовими особами, діяльність яких, імовірно, ще пов'язана з якістю протиепідемічних заходів.

Картина розвитку епідемій в різні роки є якісно подібною. Це більш наочно, якщо відкинути період 2009-2010 років, в якому додалась епідемія якісно нового виду грипу (свинячий грип) (рис. 3.14). По вісі ординат відкладена кількість захворілих на 10 тис. населення I_{WEEK}. По вісі абсцис - номери тижнів n_{WEEK}, які відліковуються з середини літа (27 тиждень року – перша декада липня), коли рівень захворюваності мінімальний.

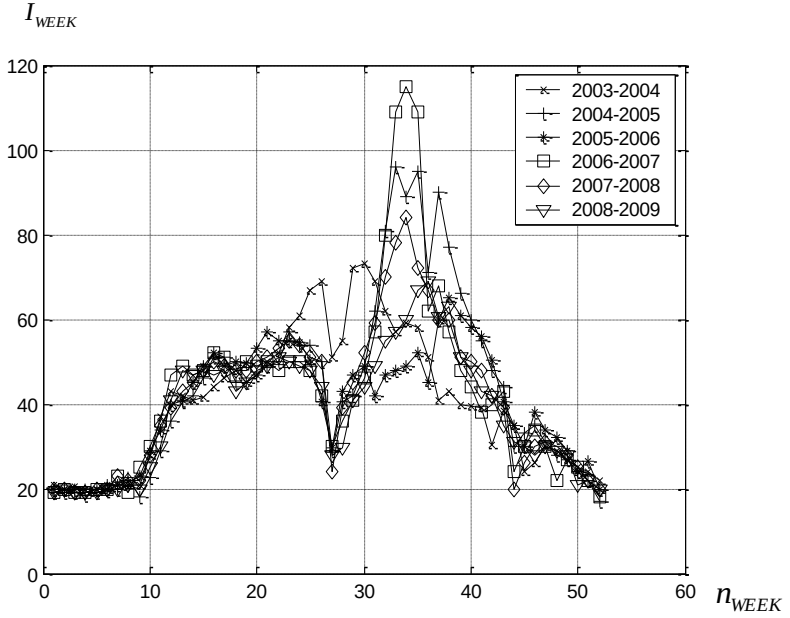


Рис. 3.14. Рівень захворюванності на грип в Україні в 2003-2009 роках

Статистичні дані [39] усереднені за десятьма містами України. Картина щодо окремого міста може бути дещо іншою. Вона може бути простішою за рахунок того, що всі процеси відбуваються в одному регіоні (за умови зменшення часу на передачу інфекції всередині регіону). Крім того, більш простою може виявитись загальна епідеміологічна картина України через усереднення даних від різних міст. Визначення домінуючої тенденції вимагає додаткових досліджень.

Як бачимо, кожного року хід епідемії має декілька характерних етапів: першу та другу хвилю, які, в свою чергу, складаються з декількох малих хвиль. Практично кожного року друга хвиля за рівнем більше першої. Дещо відрізняється епідемія 2009-2010 років, яка мала дві великі хвилі, але їх амплітуда та частота виникнення були набагато більшими, що, вірогідно, повязано з принципово новими властивостями збудника захворювань, вивчення яких також доцільно винести в окреме дослідження. Типовою можна вважати картину розвитку епідемії грипу 2008-2009 років (рис. 3.15), в якій амплітуда першої хвилі майже в півтора рази менше амплітуди другої.

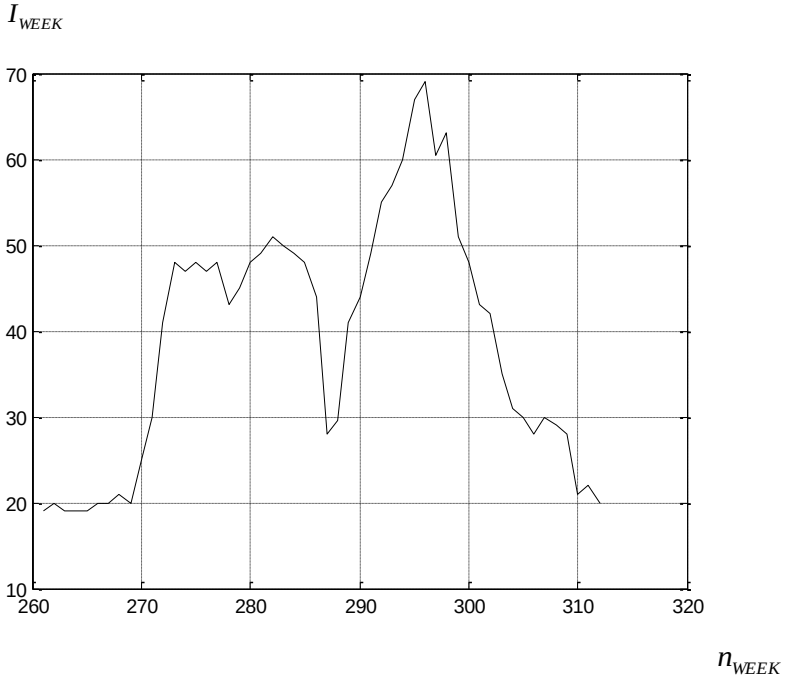


Рис. 3.15. Рівень захворюванності на грип в Україні в 2008-2009 роках, як найбільш типовий в періоді 2003-2009 років

В інші роки цього ж періоду амплітуда другої хвилі перевищує амплитуду першої на 10 - 125%. Початок цієї хвилі пов’язаний з різкою

зміною погодних умов: збільшення вологості (опади), зменшення температури навколишього середовища; та з недостатньою адаптацією організму людини до нових погодних умов. До того ж висока вологість (опади) має більший вплив на захворюваність, ніж просто низька температура. Низька температура при низькій вологості викликає захворювань набагато менше.

Захворюваності також сприяє відсутність адаптації організму до осінньо-зимових умов. На жаль, адаптація організму людини при переході від теплої пори року до холодної не формується миттєво і не може бути сформована заздалегідь. Авансом можна виконувати загальне загартовування організму, яке необхідно враховувати окремо від адаптації. Залежність ступеня адаптації до нових погодних умов від часу має S-подібний характер, наближений до логістичного [39]. На рис. 3.16 t – час, y – ступінь адаптації, Y_{min} – початковий рівень адаптації, Y_{max} – максимально можливий рівень адаптації, до якого йде асимптотичне наближення.

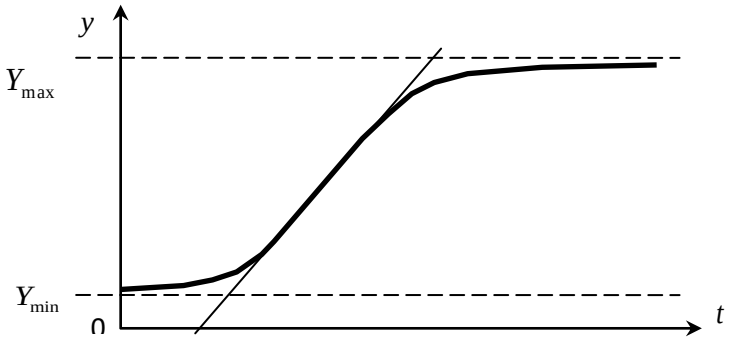


Рис. 3.16. Графік логістичної функції зростання

Епідемії не виникають миттєво у всіх географічних місцях. На передачу збудника та на його поширення новою територією потрібен деякий час [7]. Загальний вид окремої хвилі захворювань під час епідемій промодельований у роботах [9, 51].

Оскільки модель стосується географічно обмеженого регіону, то, виходячи зі специфіки процесу збору статистичних даних, хвилі епідемії є сумою окремих хвиль в різних містах України (рис. 3.17). Крім того, може виявитись, що це взагалі одна хвиля епідемії, яка була зафіксована в різних містах, показники якої були просумовані подібно (рис. 3.17).

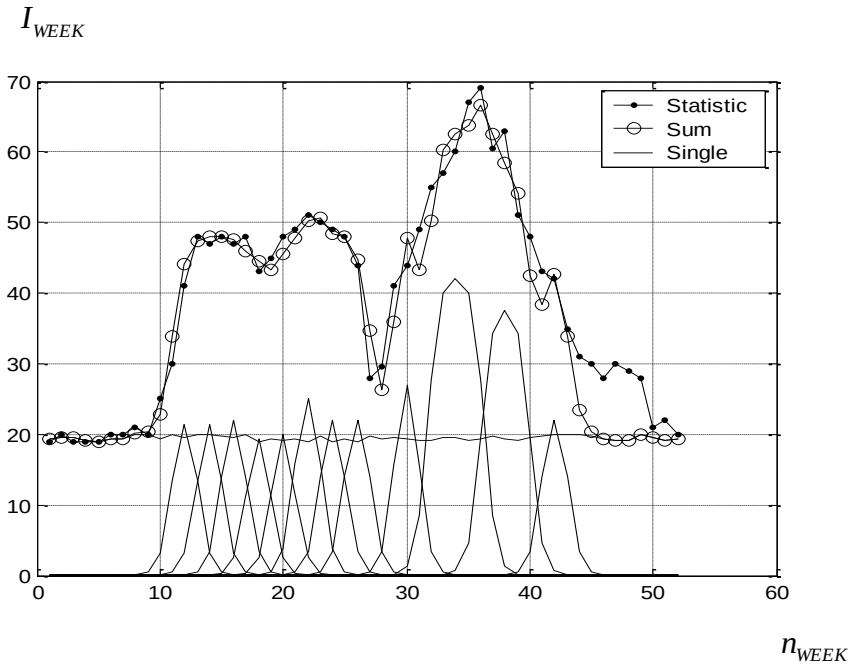


Рис. 3.17. Рівень захворюванності на грип в Україні в 2008-2009 роках та його складові по різних містах
(Statistic – крива за даними статистики, Sum – сума модельних показників за окремими містами, Single – модельні показники рівня захворюваності в окремих містах та мінімальний річний рівень захворюваності по всій Україні, який дорівнює 19-20)

До заходів, які розбивають епідемію на декілька хвиль, може також належати вакцінація, карантинні заходи, шкільні каникули, тривалі святкові дні. Важливим фактором впливу на сприйнятливість до

інфекції є стан організму, зокрема імунітет. Повноцінне харчування, сон та відпочинок сприяють зменшенню сприйнятливості до інфекції.

З організаційної точки зору активні та пасивні протиепідемічні заходи стають ефективнішими з часом, а не відразу після оголошення загрози епідемічного стану. Мало спланувати правильні протиепідемічні заходи – їх ще треба виконати. А виконувати ці дії набагато легше, коли не лише лікар, але й населення бачить реальну небезпеку захворювань. Зростання ефекту протиепідемічних заходів у часі відбувається за S-подібною залежністю.

Однією з задач прогнозування є ідентифікація параметрів математичних моделей за допомогою статистичних даних. Чисельне моделювання [51] дозволяє спрогнозувати рівень епідемії залежно від величини ключових параметрів.

Одним з важливих протиепідемічних заходів є вчасне виявлення моменту початку різних стадій епідемії та оперативне визначення типу збудника, його властивостей з метою подальшої побудови оптимальної стратегії протидії.

В залежності від поточних умов, можливостей та вартості вище перелічених заходів діагностики та профілактики приймається рішення щодо їх застосування. В математичних моделях прогнозування захворювань інформація щодо комплексу виконаних протиепідемічних заходів є основою формування відповідних коефіцієнтів математичної моделі.

Аналогічний аналіз був проведений щодо динаміки розвитку екологічних процесів, в результаті якого також був зроблений висновок про найбільшу адекватність логістичних моделей розвитку [52].

3.3. Використання епідеміологічного підходу до прогнозування інцидентів інформаційної безпеки

3.3.1. Огляд класифікації станів об'єктів моделювання

Для класифікації моделей комп'ютерних епідемій узагальнимо дані від різних авторів стосовно характеристик (станів) об'єктів, на які можуть впливати шкідливі фактори (віруси, помилки тощо):

P (Population) – загальна кількість населення (популяції) [6]. В [88] позначений як N (Number);

N0 (Not susceptible**)** – несприйнятливі до зараження ще до початку епідемії внаслідок відсутності об'єкта в зоні зараження або внаслідок дуже високого рівня захисту від зараження (позначення введено автором). В [92] позначене, як M (passive iMmunity);

S (Susceptible) – здоровий і сприйнятливий щодо зараження [25];

E (Exposed) – доступний, незахищений [25]. У біологічних інфекцій – стан інкубаційного періоду. У комп'ютерних системах стан, в якому шкідливе програмне забезпечення запустило в інформаційну систему агента, який можливо нічого зловмисного не робить, але за основну мету має на наступних етапах надати доступ до системи основному шкідливому коду. В [101] позначений, як L (latent);

n – кількість стадій інкубаційного періоду [4] (рис. 3.18);

B (Breakingout) – проявлення зараження [101]. В [106] позначене, як A (Active);

D (Detected) – вже виявлена наявність шкідливого коду, але протидія поки ще не почалась [25];

I (Infected) – заражений [25];

Рис. 3.18. Стадії інкубаційного періоду

m – кількість стадій (клінічних форм) інфекційного захворювання [4] (рис. 3.19). Підхід Барояна-Рвачева передбачає n стадій інкубаційного періоду та m стадій (клінічних форм) інфекційного захворювання. Різні стадії інкубаційного періоду та стадії розвитку інфекційного захворювання краще описати за допомогою безперервних або дискретно-безперервних рівнянь. Це забезпечить цілісність дослідження.

Рис. 3.19. Стадії інфекційного захворювання **I**

Q (Quarantine) – карантин [101];

P (Patched) – вдосконалений щодо усунення виявлених вразливостей [103]. Специфіка полягає в тому, що корисні дії, щодо усунення вразливостей при масовому застосуванні в мережі можуть призводити до перенавантаження мережі, тобто до втрати функціональної стійкості типу «відмова в обслуговуванні» (DoS, Denial of Service);

N1 (Not susceptible) або R (Removed, Recovered) - вилікуваний та більше не сприйнятливий до зараження (отримав імунітет). Унікальною, що не перетинається з іншими позначками, є назва N1 (введено автором). Але в багатьох роботах поширена позначка R [25]. Тому, якщо виключене хибне тлумачення, то позначка R є більш звичною, але якщо можливе змішування понять, то кращою є позначка N1. Рідше використовуються позначки A (Antidot, Antivirus) [87] (забезпечений антивірусом) та M (iMmune) [66, 103] (отримав імунітет);

F (Fatal) – загиблі від ускладнень [4]. Для інформаційних систем – вузли, які не підлягають відновленню протягом життєвого циклу інформаційної системи.

3.3.2. Основні види моделей комп'ютерних епідемій

Використовуючи наведені можливі стани об'єктів інформаційної системи розглянемо основні види моделей комп'ютерних епідемій. Для графічного представлення моделей будемо використовувати ланцюги Маркова, які визначають можливі переходи між станами. Коло з позначкою відповідає певному стану. Стрілки позначають напрямки можливих переходів. Закономірність переходів описують рівняння Колмогорова у вигляді звичайних диференційних рівнянь.

В даний час відомо кілька різновидів математичних моделей динаміки розповсюдження комп'ютерних вірусів на основі біологічних підходів, які різняться областю обмеження та умовами застосування в реальних програмно-технічних системах. Серед них можна виділити такі моделі: SI (Suspected-Infected), SIR (Suspected-Infected-Recovered), SEIQR (Suspected-Exposed-Infected-Quarantined-Recovered), PSIDR (Progressive Suspected-Infected-Detected-Recovered); вони здебільшого відрізняються типами і кількістю станів об'єктів зараження (незаражені; заражені, які заражують інших; заражені, які не заражують інших; вилікувані з набуттям імунітету; ті, що знаходяться у карантині, тощо), що враховуються в моделі, а також функціями переходів між цими станами, які описуються диференціальними рівняннями.

SI. Вважається, що об'єкт може бути або сприйнятливим до захворювання S, або хворим I (рис. 3.20). Лікування та одужання ця модель не передбачає. Залежно від того, чи існує верхнє обмеження на кількість хворих, модель поділяється ще на 2 підвиди.

SI exp – експоненційний розвиток. Кількість хворих може зростати нескінченно.

SI SL – розвиток має S-подібний (логістичний) характер. Кількість хворих обмежена кількістю об'єктів, що можуть бути заражені (розмір популяції, кількість комп'ютерів в мережі або

пропускна спроможність мережі щодо поширення зараження, як це було, наприклад, за хробаком Sapphire Worm).

SIS. Об'єкт може одужати (позбавитись від інфекції), але імунітету при цьому не набуває та знову переходить до стану S (рис. 3.21).

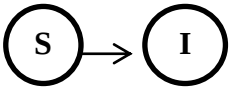


Рис. 3.20. Модель епідемії **SI**

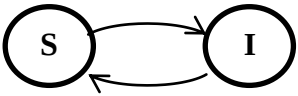


Рис. 3.21. Модель епідемії **SIS**

SIR (Kermack and McKendrick, 1927) [74]. Об'єкт не тільки позбавляється зараження, але й отримує імунітет R [14, 47] (рис. 3.22).

SIR b(t) – (Zhow, Gong, Towsley (MTI)) [25]. В цій варіації коефіцієнти, що визначають перехід від стану S до стану R є змінними у часі b(t).

SIRI (Stollenwerk, Jansen, 2011) [97]. Об'єкт позбавляється інфекції, але імунітет отримує лише частка об'єктів R, а інша може знову бути зараженою (рис. 3.23).

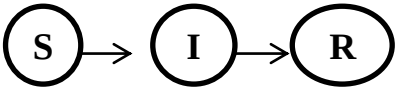


Рис. 3.22. Модель епідемії **SIR**

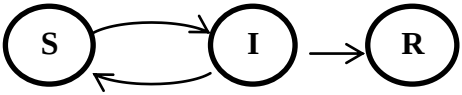


Рис. 3.23. Модель епідемії **SIRI**

SEIR. Додається латентний (прихований) період розвитку інфікування (стан **E)**, коли зараження вже відбулось, але активних дій інфекція поки що не робить (рис. 3.24). В [103, 105] аналогічну модель називають SLBS.

SEnImRF [4]. В моделі SEIR додатково враховані кількість стадій інкубаційного періоду n та кількість стадій (клінічних форм) інфекційного захворювання m. Також введений стан F для позначення повністю втрачених об'єктів (померлих) (рис. 3.25).

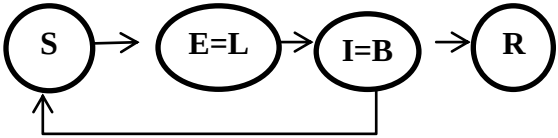


Рис. 3.24. Модель епідемії **SEIR (SLBS)**

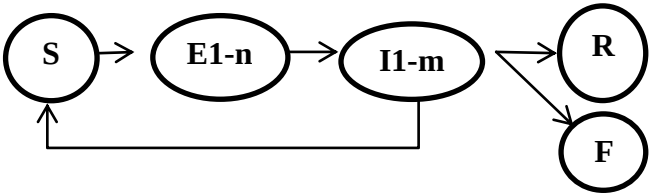


Рис. 3.25. Модель епідемії **SEnImRF**

SLBQRS [101]. В модель SEIR (SLBS) додане витримування об'єктів у карантині Q (рис. 3.26).

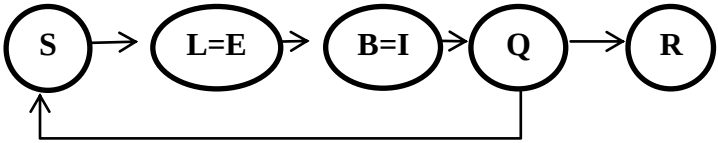


Рис. 3.26. Модель епідемії **SLBQRS**

SIPS [13, 89]. Враховані витрати машинних ресурсів (зокрема часових) для «накочування латок» на вразливості програмних систем (рис. 3.27). Пунктиром показаний стан, який за логікою має бути присутній, але в назві моделі не відображений.

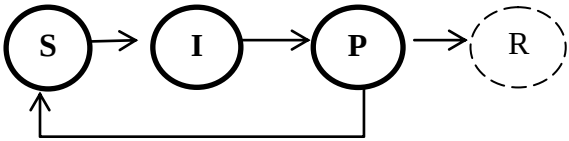


Рис. 3.27. Модель епідемії **SIPS**

PSIDR [76]. Progressive SIDR окремо розглядає стан детектування (виявлення) D зловмисного коду та динаміку реакції системи на небезпеку, що є виявленою. Цю модель ще називають моделлю з протидією [25]. Процедура є двоетапною. Спочатку система працює, як модель SI, а на другому етапі – як модель SIDR (рис. 3.28).

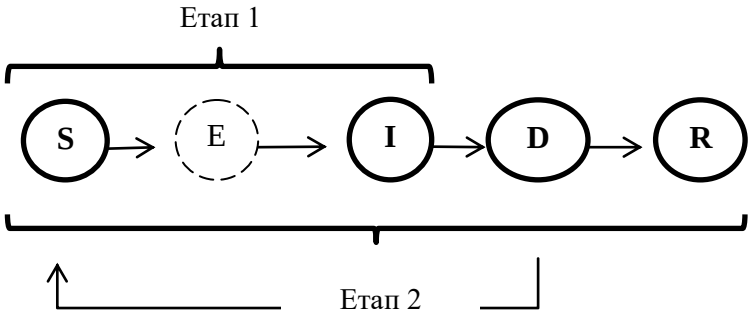


Рис. 3.28. Модель епідемії SIDR

Деякі моделі отримали назву від особливостей дій зловмисного коду. Наприклад, за ознакою інтелектуального вибору наступних адрес зараження виділяють моделі AAWP (Analytical Active Worm Propagation) активного аналітичного поширення хробака та RCS (Random Constant Spread) поширення за випадковою константою. При цьому загальна модель системи протидії може бути будь-якою з перелічених вище.

Еволюція розглянутих моделей на початкових етапах відбувалась в однаковій послідовності як для біологічних, так і для комп'ютерних епідемій. Далі відмінності фізичної сутності об'єктів призвели до суттєвої різниці у напрямках розвитку моделей (рис. 3.29).

Ці моделі поширення комп'ютерних вірусів мають низку загальних недоліків, зокрема не враховують топологію, у тому числі зв'язність комп'ютерної мережі, та часові затримки як всередині кожної комп'ютерної локальної мережі, так і між мережами [25, 30, 57, 66, 76]. Окрім того, кожна модель має й власні недоліки й особливості.

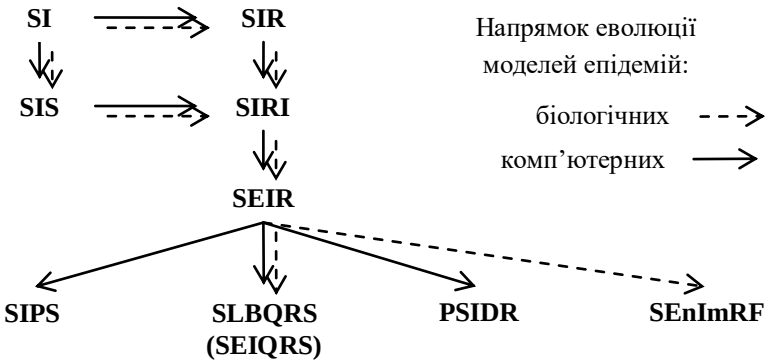


Рис. 3.29. Еволюція моделей епідемій

Так, наприклад, характерною особливістю моделі SI є нехтування антивірусним ПЗ, що призводить до безповоротності епідемічного процесу в комп'ютерних системах.

В моделі SIR не враховується те, що у реальних умовах для лікування комп'ютерних систем існує необхідність ідентифікації і локалізації зловмисного ПЗ. Ця процедура вимагає певних (від частки секунди до десятка годин) часових витрат. Це також знижує сферу застосування вказаної моделі.

Водночас модель PSIDR зорієнтована на усунення одного з недоліків моделі SIR через розбиття моделі поширення комп'ютерних загроз на два етапи, введення затримки між початками цих двох етапів, ідентифікації, локалізації та лікування зловмисного ПЗ, що дає можливість незалежного аналізу процесу зараження та лікування.

3.3.3. Розвиток існуючих моделей щодо набору станів об'єктів

Далі розглянуті основні напрямки вдосконалення існуючих моделей епідемій, які дозволяють підвищити адекватність моделювання.

1. Розширення та систематизація набору типів станів **S.**

Деякі автори вже намагались це робити, але ці стани визначались як принципово нові R (Removed, Recovered) [87], D (Delay) [104] і не пов'язувались між собою, хоча насправді вони є окремими випадками стану **S.** Тому пропонується ввести такі підтипи стану **S:**

S1 – сприйнятливість до первинного зараження.

S2 – сприйнятливість до зараження після того, як був вилікуваний (не отримав імунітет). В [87] позначений як R (Removed, Recovered).

S3 – сприйнятливість до зараження після того, як був вилікуваний (отримав імунітет), але через певний час з'явилась нова модифікація вже відомої інфекції. В [104] позначений як D (Delay), оскільки стає знов сприйнятливим після затримки у часі, яка потрібна для модифікації інфекції.

2. Стани **B** (breakingout) [101] проявлення зараження та **D** (Detected) [25] виявлення наявності зараження без активної протидії можна вважати еквівалентними. Оскільки термін «проявлення» зараження завжди розглядається з точки зору системи спостереження (на базі людей, техніки, людино-машинних систем). Якщо система спостереження вважає, що зараження «проявилось» **B**, значить наявність зараження вже «детектована» **D**. Тому пропонується замість двох станів **B** і **D** використовувати єдиний стан **D.**

3. Стан **I** передбачає проведення лікування, використовуючи зовнішні ресурси, або самоодужання об'єкту завдяки власним ресурсам. Інакше об'єкт зі стану **I** ніколи не перейде до іншого стану. Отже, для стану **I** обов'язково потрібно враховувати застосування засобів лікування для кожної стадії окремо (**I1, I2, … Im**) [25]. Для узагальнення підходу у разі відсутності лікування вважатимемо, що воно дорівнює нулю.

4. Спостереження, збір інформації є підготовчою стадією будь-якого лікування. З урахуванням того, що стан **I** може містити декілька стадій, стани **B** і **D** можуть бути занурені в першу стадію - стан **I1.** Тобто на початковій стадії проявлення зараження система протидії тільки спостерігає та збирає інформацію для подальшого обрання найбільш ефективних засобів протидії.

З урахуванням запропонованих змін щодо класифікації та розширення набору можливих станів об'єктів, узагальнимо всі можливі стани в табл. 3.2.

Таблиця 3.2

Позначення станів об'єктів зараження у різних авторів

Автори, моделі	**Позначки станів об'єктів моделі**														
Узагальнені та запропоновані в даній роботі, **NF**	**P**	**N0**	**S1**	**S2**	**S3**	**E**	**n**	**B**	**D**	**I**	**m**	**Q**	**P**	**N1**	**F**
Kermack, McKendrick, 1927, SIR															
Kephart, Whites, 1991, SIS															
Бароян, Рвачев, 1977, SEnImRF	P		S X			E	n			I Y	m			R	F
Cohen, 1985															
Garetto, Gong, Towsley, 2003, SIR			S							I				M	
Serazzi, Zanero, 2003, MSEIR		M	S			E				I				R	
Боєв, 2004, SEIRF	P		S			E				I				R	F
Боєв, 2005, SEIR SEnImRF	P		S X			E	n			I Y	m			R	F
Martcheva, 2005, SIS, SIR	N		S	R						I					
Britton, 2009, SIS, SIR, SEIR, SIRS			S			E				I				R	
Монахов, Груздева, Монахов 2010, SI, SIS, SIR, PSIDR			S			E			D	I				R	
Stollenwerk, Jansen, 2011, SIS, SIR, SIRI			S							I				R	
Климентьев, 2013, SI, SIS, SIR, SEIR, SIRS, PSIDR			S	S		E			D	I				R	
Yang, Yang, Wu, 2017, SLBS, SIPS			S	S				B		I			P		
Zhang, Wang, Ferrara, SEIQRS з затримками			S	S		E				I		Q			
Zhang, Song, 2017, SLBRS з затримками			S			L		A						R	
Umbreen, Mubasher, Nauman, Malik, 2018, SLBQRS			S	S		L		B				Q		R	
Onwubuoya, Akinuemi, Odabi, Odachi, 2018, SIRS	N		S	R						I				A	
Yao, Fu, Yang, Wang, Sheng, 2018, SIQVD			S		D					I		Q		V	
Champredon, Dushoff, Earn, 2018, SEIR			S			E				I				R	

На основі проведеного аналізу існуючих моделей та з урахуванням пропозиції щодо підвищення адекватності побудови окремих елементів моделі побудуємо вдосконалену загальну модель епідеміологічного процесу (рис. 3.30). Як було показано вище, зазвичай моделі епідемії називають за літерами, що позначають основні стани об'єктів. Для нашої моделі назва, яка сформована таким чином, була б занадто довгою (SEIBDPQNF). Тому назвемо модель за першими літерами стаціонарних станів, що виникають після закінчення епідемії – NF (де N – здорові, F – померлі).

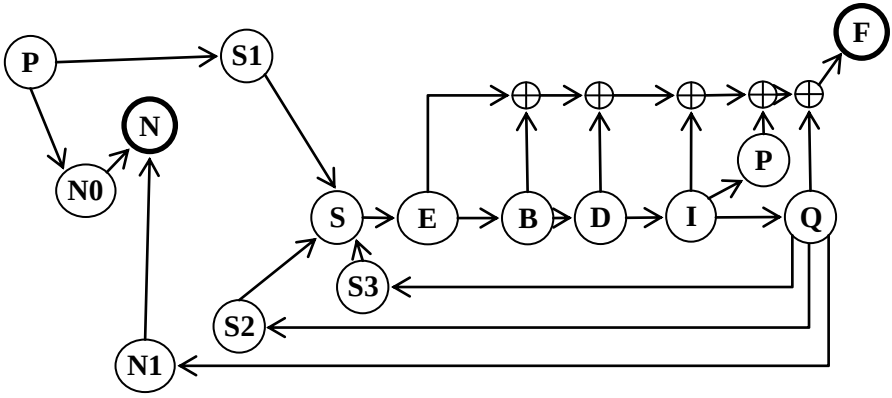


Рис. 3.30. Загальна **NF** модель епідеміологічного процесу

Як відомо, моделі комп'ютерних епідемій були отримані шляхом адаптації (трансформації) моделей біологічних епідемій до особливостей комп'ютерних об'єктів. Логіка взаємних трансформацій між біологічними та комп'ютерними моделями епідемій представлена на рис. 3.31.

Стани N, S, E, I, F спочатку були запропоновані в біологічних моделях епідемій, потім були адаптовані для моделей епідемій комп'ютерних. Стани B, D, навпаки, спочатку з'явились у моделях епідемій комп'ютерних, а потім у біологічних. Стани P, Q з'явились у моделях епідемій комп'ютерних та біологічних практично незалежно один від одного.

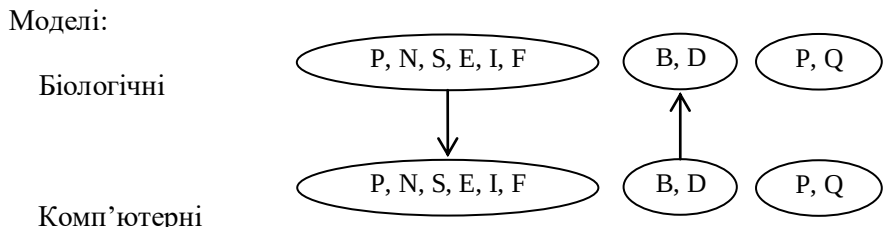


Рис. 3.31. Еволюція станів у моделях епідемій

Для інтегрування диференціальних рівнянь, що входять до складу розглянутих моделей найчастіше використовують такі методи:

NSFD (nonstandard finite difference) [101];

FD (finite difference) – кінцевих різниць Ейлера.

RK-4 (Runge-Kutta) – Рунге-Кутта 4-го порядку.

EPC (Euler Predictor Corrector) – метод Ейлера з корегуванням на основі передбачення [87, 76, 53].

Стани S (S1, S2, S3), N0, N1 (R), P виникають при використанні контрзасобів. Класифікуємо основні групи контрзасобів. Для цього розширимо висновки стосовно основних можливих контрзасобів щодо атак [80] даними до відповідних моделей та основних технічних засобів:

1. Моніторинг та раннє попередження (модель SI). Контрзасіб IDS (Intrusion Detection System) – системи виявлення проникнення.

2. Очищення та дезінфекція вузлів (SIR). Контрзасоби - антивіруси.

3. Карантин, що визначений як найстаріший засіб захисту, дозволяє убезпечити інші вузли мережі, більш точно визначити вид інфекції та підібрати найбільш адекватні засоби протидії (SEIQRS).

4. Імунізація. Контрзасіб IPS (Intrusion Prevention System) – системи випередження проникнення.

5. Горщик з медом та смоляна яма (заманювання зловмисного коду на спеціально підготовлені об'єкти з метою затягування часу задля вивчення та підбору ефективних засобів протидії).

6. Контратаки та «гарні» хробаки.

Хробаки-антивіруси за видами активності на різних етапах розвитку можна класифікувати у такий спосіб [25]:

Етап пошуку цілей

A (Active) – активне сканування адресного простору, наприклад, випадковим чином.

P (Passive) – пасивне очікування спроби нападу з іншого вузла і тільки після цього контратака.

Етап розмноження

S (Susceptible) – заражає тільки здорові об'єкти.

I (Infected) – заражає об'єкти, на яких присутні «погані» хробаки.

Етап боротьби з «поганим» хробаком

R (Remote) – видаляє «поганого» хробака з об'єкту.

V (Vaccinate) – вакцинує об'єкт, робить його несприйнятливим для подальшого зараження.

3.3.4. Розвиток існуючих моделей на основі логістичних моделей

Як вказувалось, попередні дослідження показали, що найбільш адекватними серед моделей розвитку є логістичні моделі. Справа у тому, що практика висуває до моделей суперечні умови [50]: оперативність, точність, наочність, повнота врахування чинників впливу тощо. Складність моделі має відповідати складності процесу та, крім того, можливості щодо забезпечення вхідними даними. Чим складнішою є модель, тим складніше забезпечити її вхідними даними, і тим вищим є ступінь невизначеності, в якій вона функціонує. Моделювання розвитку епідемій слід починати із грубих моделей. Переваги грубих моделей: оперативність підготовки до застосування (оперативність структурного та параметричного синтезу), наочність, простота вчасного корегування параметрів відповідно до зміни внутрішніх та зовнішніх умов дії об'єкту моделювання.

Якщо ресурсне забезпечення варіюється довільно або розглядається декілька етапів життєвого циклу, то більш адекватною є S-подібна логістична модель [50, 53] у вигляді звичайного диференціального рівняння

$$\frac{dy}{dt} = m \cdot (y - Y_{min}) \cdot (Y_{max} - y), \quad (1)$$

або у вигляді функції, що є його розв'язком:

$$y(t) = Y_{min} + \frac{Y_{max} - Y_{min}}{1 + e^{-m \cdot (Y_{max} - Y_{min}) \cdot (t - \Delta t)}}, \quad (2)$$

де y – динамічна змінна розвитку (наприклад, кількість інфікованих); t – час; Y_{min}, Y_{max} – нижнє та верхнє обмеження величини y; m – постійний коефіцієнт; Δt – абсциса точки симетрії (зсув кривої вздовж вісі абсцис).

Для моделювання епідемій найкраще підходящими вважаються інтегрально-диференціальні рівняння [6, 8, 94, 95]. Вони є математично чіткими, але не дуже зручні у використанні.

Крім того, проміжні результати їх розв'язання інколи недостатньо наочні для фахівця з управління інформаційною безпекою (або системного адміністратора) без спеціальної математичної підготовки. В роботі [94] для спрощення моделі був виконаний перехід до логістичних звичайних диференціальних рівнянь в кінцевих приростеннях та заміна інтегрування кінцевими сумами.

Модифікуємо відому структурну модель Б.В. Боєва [6] (рис. 3.32).

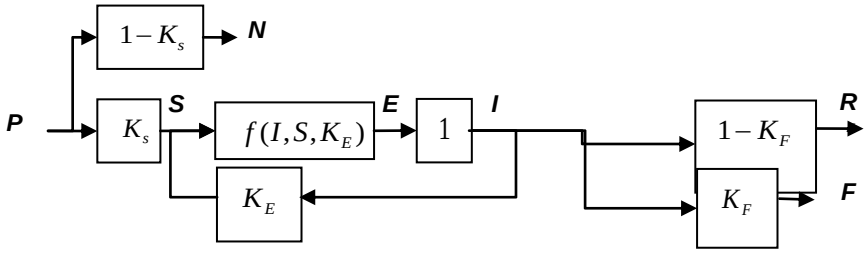


Рис. 3.32. Модифікована структурна модель епідемії Боєва Б.В.

В цій моделі позначено: P – загальна кількість об'єктів зараження, S, N – сприйнятливі та несприйнятливі до зараження, E – в інкубації (заражені самі, але поки що не заражають інших і не ідентифікуються), I – заражені об'єкти, які активно заражають інших, R ($N1$) – об'єкти, які вилікувані та отримали імунітет (завдяки антивірусу), F – об'єкти, які довелося повністю вилучити з роботи після зараження; K_S, K_E, K_F – коефіцієнти, відповідно, сприйнятливості до зараження, передачі зараження, вилучення з роботи (повна втрата працездатності); $f(I,S,K_E)$ – логістична залежність зараження з числа сприйнятливих.

Розглянемо більш детально математичні залежності переходів між станами об'єктів.

Спочатку знаходимо початкові кількості об'єктів несприйнятливих та сприйнятливих до зараження: $N_0 = P \cdot (1 - K_s)$, $S_0 = P \cdot K_s$.

Знайдені величини приймаються як початкові умови станом на початковий момент часу t_0. Надалі кількість об'єктів несприйнятливих до зараження може корегуватись коефіцієнтом K_S, який відбиває природну несприйнятливість (особливості операційної системи), несприйнятливість, яка була сформована через антивірусні засоби, повну ізоляцію частки об'єктів за допомогою карантинних заходів тощо. Але дія коефіцієнту 1 - K_S стосовно переведення об'єктів до групи несприятливих буде стосуватись лише тієї кількості сприйнятливих об'єктів S, які не перейшли до інших груп (E , I , R , F). Якщо в якийсь момент часу t_i (внаслідок вжитих випереджувальних заходів) кількість несприйнятливих об'єктів збільшилась на величину ΔN, то загальна кількість несприйнятливих об'єктів на момент часу t_i буде обчислюватись як сума попередньої величини N та відповідного прирощення $N(t_i) = N(t_{i-1}) + \Delta N(t_i)$.

Встановлюємо крок інтегрування рівнянь за часом рівним Δt та починаючи з початкового моменту часу t_0 на кожному кроці послідовно обчислюємо зміни станів об'єктів. Диференціальне рівняння зростання

кількості об'єктів, які знаходяться на першому часовому проміжку - в інкубаційному періоді, записуємо в кінцевих різницях $\frac{\Delta E_1}{\Delta t} = K_E \cdot I \cdot S$.

Остання залежність є подібною до одного з рівнянь Лоткі-Вольтерри. Розв'язком рівняння (з урахуванням складної взаємодії з іншими змінними) є залежність, яка якісно подібна до логістичної. Знайдемо величину прирощення кількості об'єктів, які знаходяться в стані першого періоду часу інкубаційного періоду $\Delta E_1 = K_E \cdot I \cdot S \cdot \Delta t$.

Після цього зменшуємо кількість сприйнятливих об'єктів на знайдену величину $S = S - \Delta E_1$.

Оскільки інкубаційний період T_E та період стану зараження T_I більше кроку інтегрування Δt, то введемо для змінних E, I нижні індекси, які будуть позначати номер проміжку часу в періоді інкубації або стану зараженості (наприклад, якщо Δt дорівнює хвилині, то це номер хвилини у відповідному періоді):

$$E_i,\ i = \overline{1, i_{end}^E},\quad I_i,\ i = \overline{1, i_{end}^I},$$

де $i_{end}^E = \frac{T_E}{\Delta t}$, $i_{end}^I = \frac{T_I}{\Delta t}$ - номери останніх проміжків часу у відповідних періодах.

Далі виконується зсув стану заражених об'єктів. Всі ті, що були в стані $(i-1)$-го проміжку часу переходять у стан (i)-го проміжку часу $E_i = E_{i-1},\ i = \overline{1, i_{end}^E - 1}$.

Ті, хто був на останньому проміжку часу інкубаційного періоду i_{end}^E, переходять на перший проміжок часу стану інфікування $I_1 = E_{end}$.

Далі аналогічним чином виконується процедура зсуву станів інфікованих об'єктів $I_i = I_{i-1},\ i = \overline{1, i_{end}^I - 1}$.

Загальна кількість об'єктів інфікованих та в інкубаційному періоді знаходяться як відповідні суми заражених об'єктів на всіх часових проміжках відповідних періодів:

$$E = \sum_{i=1}^{i_{end}^{E}} E_i \,,\; I = \sum_{i=1}^{i_{end}^{I}} I_i \,.$$

Прирощення кількості об'єктів, які вилікувані, та об'єктів, які довелось вилучити з роботи, знаходяться за відповідними коефіцієнтами стосовно кількості заражених об'єктів, що є на останньому часовому проміжку зараження:

$$R = K_R \cdot I_{end} \,,\; F = (1 - K_R) \cdot I_{end} \,.$$

Реалізація моделі в програмному середовищі MATLAB підтвердила її працездатність та адекватність (рис. 3.33).

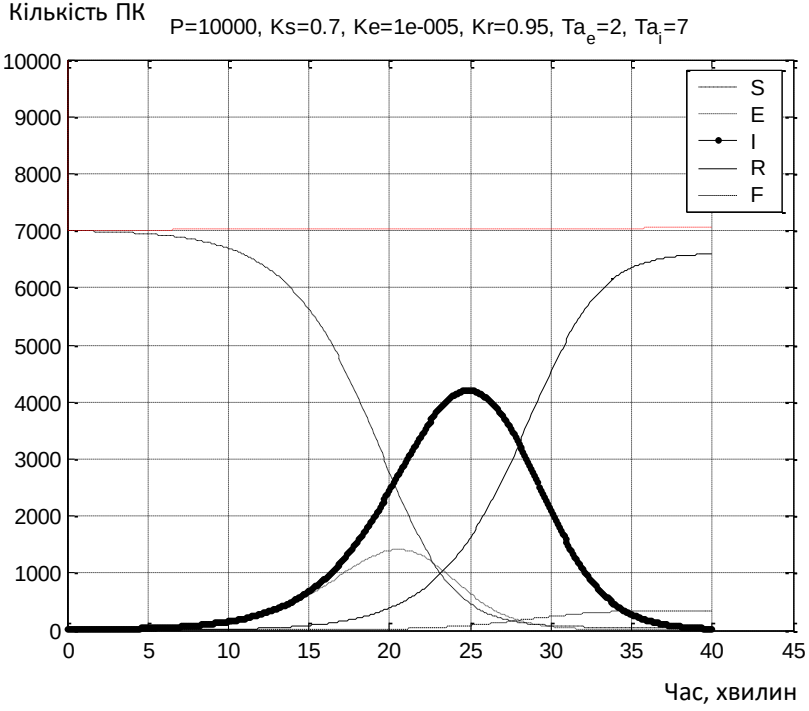


Рис. 3.33. Результати чисельного моделювання кібератак

Часова шкала відрізняється для різних видів інформаційних та кібератак. Основна увага приділена багатоетапним або багаторівневим атакам. Тому в моделі залишили суто біологічну характеристику – інкубаційний період. Інкубаційний період в комп'ютерному світі відповідає латентному періоду, під час якого зловмисний код виконує доналаштування, додаткові проникнення в умовах повної скритності своїх дій. У багаторівневій атаці зловмисний код 1-го типу спочатку послаблює захист, готує віртуальні канали гарантованого доступу до інформаційних ресурсів та ресурсів керування. Потім по підготовлених каналах більш зловмисний код 2-го типу потрапляє в систему (або в іншу більш захищену чи більш контрольовану частину системи) і виконує основне зловмисне завдання. Таких рівнів атак може бути декілька. Ці рівні атак можуть поєднувати фізично різні способи атак від суто технічних до соціальної інженерії.

Під час моделювання з'ясовано, що збільшення кроку інтегрування веде до суттєвого пошкодження якісної картини розвитку епідемії (спостерігаються явища детермінованого хаосу). Зменшення практично не вносить змін ані до якісної, ані до кількісної картин процесу розвитку, але пропорційно збільшує час моделювання.

Графіки показують логістичний характер зниження кількості сприйнятливих об'єктів та зростання кількості вилікуваних об'єктів та об'єктів вилучених з роботи. Загальний вигляд залежності кількості інфікованих об'єктів та об'єктів, які знаходяться в інкубаційному періоді відповідає існуючим статистичним даним щодо розвитку біологічних епідемій, що дозволяє використовувати відомі біологічні закономірності для комп'ютерного світу. Основним практично корисним результатом моделювання є дзвоноподібна залежність кількості інфікованих об'єктів. По амплітуді цієї залежності визначають рівень небезпеки епідемії. В цьому принципова відмінність епідемій біологічного і комп'ютерного світів. У комп'ютерному світі вважається небезпечним будь-яке зараження.

Але проведемо аналогію з біологічним світом. Як відомо, в біологічному світі не буває організмів повністю вільних від

небезпечних вірусів, бактерій, паразитів або інших об'єктів, які без дозволу використовують ресурси організму. Будемо називати їх чужорідними біологічними об'єктами. Організм здебільшого або утримує певний баланс з чужорідними біологічними об'єктами, або навіть вступає з ними в співпрацю - симбіоз. Якщо знищити всі чужорідні біологічні об'єкти, то на їх місце все одно прийдуть інші, які можуть виявитись більш шкідливими. Тому в біологічному світі організм бореться не проти всіх чужорідних об'єктів. Схожа ситуація можлива і в комп'ютерному світі. Але деякі механізми працюють інакше. Наприклад, наявність корисних (точніше нешкідливих) чужорідних об'єктів не гарантує відсутності інших (більш зловмисних) об'єктів. Хоча інколи це правило працює і в біологічному світі. Крім того, на відміну від біологічного світу наявність вільного від чужорідних об'єктів простору не веде до обов'язкового його заселення іншими (зловмисними) об'єктами. Загальний висновок щодо біологічних і комп'ютерних чужорідних об'єктів – не обов'язково боротися проти всіх таких об'єктів.

Повернемось до результатів моделювання.

Моделювання показало, що *першою необхідною умовою* початку епідемії є поява певної (ненульової) кількості інфікованих або об'єктів, які знаходяться в стані інкубаційного періоду.

Виходячи з результатів моделювання, *другою необхідною умовою* виникнення епідемії є певне співвідношення частки несприйнятливих об'єктів та умов передачі інфекції від заражених до сприйнятливих об'єктів. Математично це визначається певним співвідношенням коефіцієнтів K_s та K_E.

Достатньою умовою виникнення епідемії є одночасне виникнення першої та другої необхідних умов.

При цьому під епідемією розуміють стан, коли відсоток виведених з ладу об'єктів перевищує певну величину. В технічному сенсі це величина, при перевищені якої повністю втрачає нормальну працездатність інформаційна інфраструктура певної бізнес-області (підприємство, організація, галузь).

Виходячи з цього можна зробити висновок, що головним практичним результатом моделювання є виявлення "дзвоноподібної" залежності кількості заражених об'єктів, при цьому амплітуда "дзвоноподібної" залежності визначає рівень епідемічної небезпеки. Передумовою початку епідемії є певна пропорція нестійких щодо зараження об'єктів та наявність умов передачі інфекції від інфікованих до сприйнятливих об'єктів, що визначається певним співвідношенням K_s і співвідношенням K_E.

Дослідження залежностей епідемічних піків від K_s і K_E (рис. 3.34, 3.35) корисне для прийняття рішень. Більш цінним є визначення залежностей піків епідемій від K_s і K_E одночасно (рис. 3.36, 3.37).

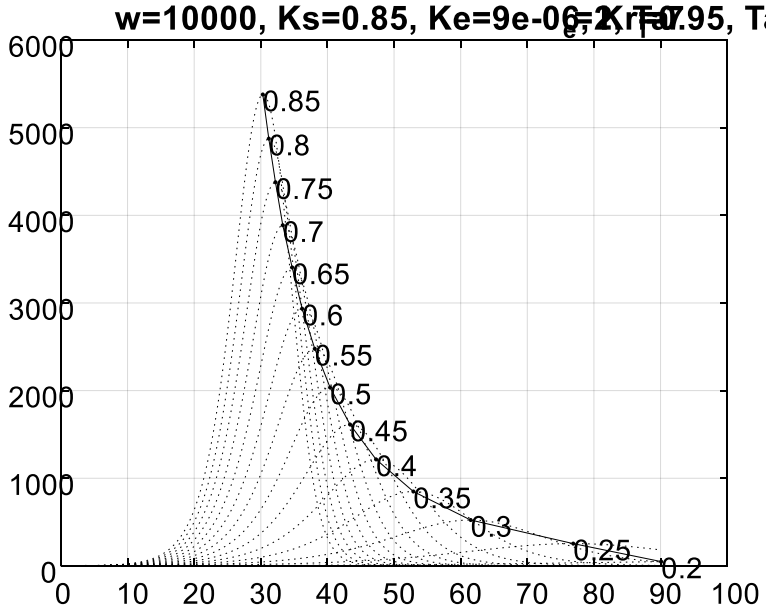


Рис. 3.34. Залежності піків епідемії від коефіцієнту сприйнятливості щодо зараження K_s

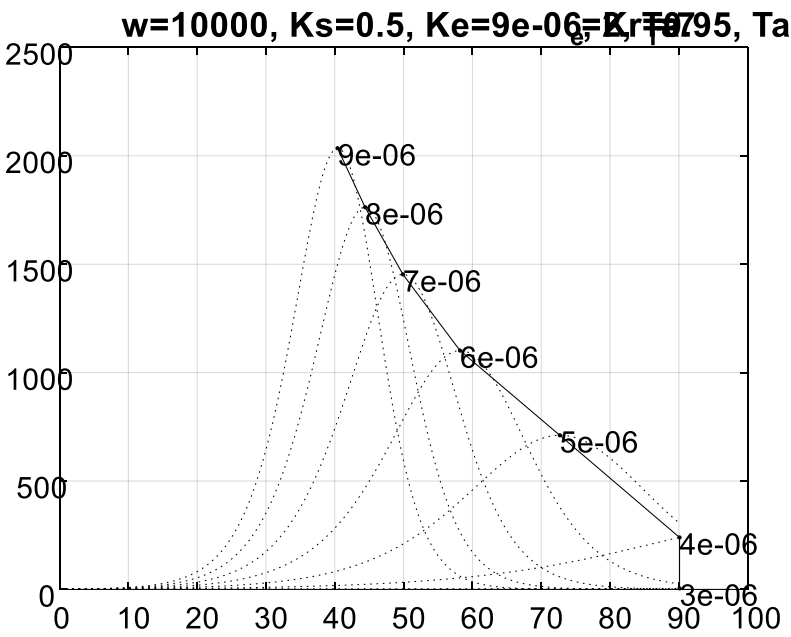


Рис. 3.35. Залежності піків епідемії від коефіцієнту передачі інфекції K_E

Якщо ми знаємо небезпечний рівень епідемічного піку, тоді ми можемо намагатися утримати в певних межах величини K_S і K_E, бо їх певні значення будуть вести до небезпечного рівня епідемічного піку у випадку виникнення інцидентів. У цьому сенсі K_S і K_E є керуючими факторами для епідемічного процесу кіберінцидентів.

Але можливе розв'язання й зворотної задачі – визначення K_S і K_E, виходячи з конкретної залежності рівня інфікування від часу. Загальний вид знайдених залежностей $K_S(t)$ і $K_E(t)$ дозволить проводити поточний та ретроспективний аналіз ефективності протиепідемічних заходів.

Проаналізуємо зміст керуючих параметрів K_S і K_E на прикладі веб-ресурсу органу управління.

Нехай на деякому комп'ютері встановлене загальне та спеціальне програмне забезпечення. Низка інших комп'ютерів в локальній мережі виконують адміністративно-господарські задачі або задачі

документообігу. Залежно від прийнятої політики безпеки, всі комп'ютери можуть працювати в автономному режимі, або бути підключеними до локальної мережі, або до мережі Інтернет. Вихід з ладу будь-якої складової обчислювального комплексу веде до втрати частки функцій органу управління.

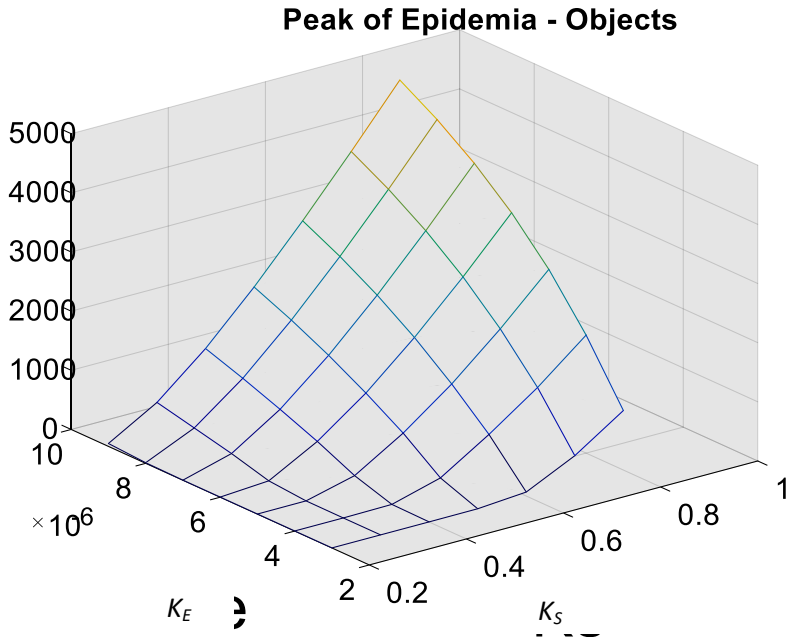


Рис. 3.36. Залежність піків епідемії від коефіцієнтів сприйнятливості K_S та передачі інфекції K_E: 3D вигляд

Проаналізуємо основні параметри процесу розвитку епідемії з погляду розглянутої мережі:

P(1- K_S) – частка вузлів мережі, які мають абсолютний захист від атак. Це досягається такими шляхами, як повне відключення від мережі та заборона використання зовнішніх носіїв інформації, які потенційно можуть бути підключені до інших комп'ютерів – 100% захист; встановлення антивірусних програм, firewall, IPS тощо – захист наближений до 100%;

K_E - показник ефективності поширення зловмисного коду по всій системі у разі, якщо десь в ній відбулось зараження.

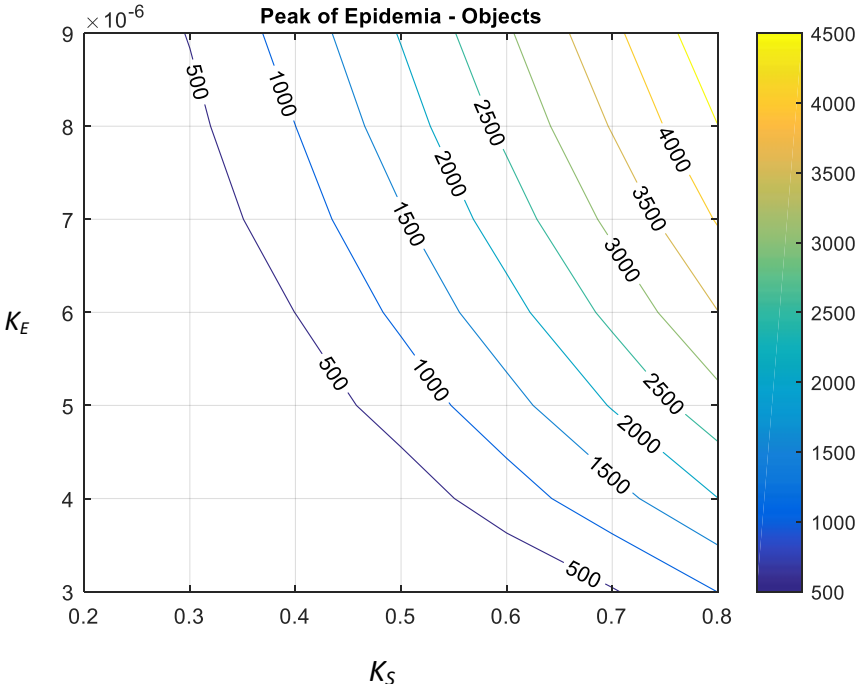


Рис. 3.37. Залежності піків епідемії від коефіцієнтів сприйнятливості K_S та передачі інфекції K_E у вигляді топокарти (ліній рівних рівнів)

Перелічені засоби також допомагають у такому разі, але проблеми можуть виникнути, якщо використано атаку принципово нового типу. У цьому разі суттєво знизять значення коефіцієнту K_E IDS-системи, які спроможні виявляти сам факт атаки за ознаками нетипової поведінки системи, навіть якщо атака такого виду відбулась вперше. Далі виконується миттєве блокування можливих шляхів поширення зараження, а заражена частина системи переводиться в режим карантину і далі вивчається, аналізується, лікується.

Також досить ефективними можуть виявитись дії організаційного характеру. Так, потрібно ретельно проаналізувати функціональність кожного з комп'ютерів та визначитись щодо мінімально можливого рівня включення його в обмін даними з іншими комп'ютерами, який ще дозволяє задовільно виконувати їх функції. Окремі комп'ютери можна повністю відключати від мережі на більшу частку робочого часу. Наприклад, опрацювання поточних облікових документів, які не вимагають миттєвого пересилання поточних даних в центральну базу даних. Наприклад, зберігання даних в центральному сховищі можна робити в чітко виділений час під контролем фахівців з безпеки. Виконання такого правила веде до суттєвого збільшення показника $P(1- K_S)$.

3.4. Таксонометричний підхід до кластеризації загроз нульового дня

Навіть якщо не вдається вчасно знайти способи захисту від загрози «нульового дня», але вдається ідентифікувати сам факт наявності цієї загрози, це дозволяє вжити запобіжних заходів. Виявлення факту наявності загрози «нульового дня» є репрезентативною інформацію для прийняття управлінського рішення щодо застосування інструментів протидії атаці.

Традиційним методом ідентифікації небезпечних ситуацій є виявлення нестандартної поведінки інформаційних процесів та об'єктів, що їх породжують. Але життя змінюється, і те, що було нормою вчора, може вже не бути таким сьогодні. Тому актуальним є створення автоматичних адаптивних систем виявлення нестандартної поведінки інформаційних об'єктів.

Найбільша кількість таких об'єктів може співпрацювати з інформаційною системою через глобальну мережу. Виникає задача оперативної їх кластеризації по групах різного ступеню інформаційної небезпеки для системи.

Виходячи зі значного об'єму інформації, високої мінливості структур та їх параметрів, бажано, щоб ця ідентифікація виконувалась з мінімальним залученням людини.

Методи кластерного аналізу широко використовують для підтримки прийняття управлінських рішень в багатьох галузях: соціальна поведінка [67], упорядкування знань [68], мобільні технології [85], інформаційні системи [83], розумні речі [78], програмне забезпечення [62, 75, 84] тощо. У нашому разі можна було б просто поділити всі контактуючі інформаційні об'єкти за рівнями інформаційної небезпеки. Але якщо об'єкти постійно змінюють моделі своєї поведінки, то складним стає питання обрання еталону, «нормальної поведінки», відносно якої необхідно визначати рівні небезпеки.

У такій ситуації доречно використати таксонометричний метод [75, 93]. Виходячи з аналізу публікацій, цей метод є більш популярним серед дослідників пострадянських країн, ніж серед інших дослідників. Адаптуємо таксонометричний метод до задачі визначення еталонів поведінки інформаційних об'єктів за ознаками інформаційної небезпеки.

Нехай є n інформаційних об'єктів, що взаємодіють з інформаційною системою. Система інформаційної безпеки веде постійний моніторинг цих об'єктів за формальними показниками, наприклад:

- частота звернень;
- об'єми обміну вхідної та вихідної інформації (за тематичними категоріями);
- кількість дій, що є легальними, але наближеними до таких, що можуть впливати на безпеку інформаційної системи;
- кількість невдалих сеансів зв'язку з небезпечною або невизначеною причиною збою;
- кількість невдалих спроб доступу (помилкові паролі, помилкові логіни);
- кількість порушень ролей та повноважень користувачів;

- кількість роботизованих звернень (та окремо всі інші дії веб-ботів);
- кількість спроб доступу до системного рівня інформаційної системи;
- тощо.

Перелік показників (факторів), що контролюються, може змінюватись відповідно до:

- цілей функціонування системи інформаційної безпеки;
- загального стану та сценаріїв розвитку інформаційної безпеки організації або в цілому галузі, держави, регіону тощо.

Нехай загальна кількість показників (факторів) дорівнює *m*.

Якщо при кластеризації нових інформаційних об'єктів дані за певними показниками відсутні, тоді для збереження працездатності наведених нижче процедур такі показники до моменту їх реального визначення вважаються рівними показникам еталону.

Після отримання першого набору показників для всіх об'єктів, що спостерігаються, створюється відповідна матриця X, де x_{ij} – значення *i*-го показника для *j*-го об'єкту:

$$X = \begin{vmatrix} x_{11} & \cdots & x_{1j} & \cdots & x_{1n} \\ \vdots & & \vdots & & \vdots \\ x_{i1} & \cdots & x_{ij} & \cdots & x_{in} \\ \vdots & & \vdots & & \vdots \\ x_{m1} & \cdots & x_{mj} & \cdots & x_{mn} \end{vmatrix}.$$

Для визначення еталону поведінки нормуємо означену матрицю X. Для цього знаходимо математичне очікування та середнє квадратичне відхилення для кожного з показників:

$$X_i = M\left[x_{ij}\right] = \frac{1}{n}\sum_{j=1}^{n} x_{ij},$$

$$D_i = M\left[x_{ij} - X_i\right]^2 = \frac{1}{n}\sum_{j=1}^{n}\left(x_{ij} - X_i\right)^2,$$

$$\sigma_i = \sqrt{D_i}.$$

За допомогою означених показників нормуємо кожен елемент первинної матриці показників

$$z_{ij} = \frac{x_{ij} - X_i}{\sigma_i}.$$

Таке перетворення перевело всі показники до єдиної міри, що дозволяє більш вільно та з більш високим ступенем адекватності порівнювати їх між собою та робити подальші перетворення.

Далі потрібно побудувати еталонний небезпечний інформацій об'єкт – точніше, створити набір еталонних показників, які й будуть прийняті як характеристики еталонного об'єкту. У класичному таксонометричному методі еталонним зазвичай вважають або найменші, або найбільші показники серед наявних.

$$Z_{i\_etalon} = \min_{j=1}^{n}(z_{ij}) \quad \text{або} \quad Z_{i\_etalon} = \max_{j=1}^{n}(z_{ij}).$$

У нашому разі так можна вчиняти, якщо показник має прямий (лінійний, а можливо нелінійний, але прямий) зв'язок з рівнем інформаційної безпеки. На жаль, дуже часто процеси виникнення інцидентів інформаційної безпеки настільки складні та нелінійні, що така міра еталону буде неадекватною.

Більш адекватною може бути міра типовості – зважене середнє *M*, себто найбільш безпечними можна вважати об'єкти з найбільш типовою поведінкою. Тобто:

$$Z_{i\_etalon} = \underset{j=1}{\overset{n}{M}}(z_{ij}) = \frac{1}{n}\sum_{j=1}^{n} z_{ij}.$$

Більш адекватним буде зважене середнє з ваговими коефіцієнтами β_j, які в оцінці будуть збільшувати вагу більш перевірених, більш надійних інформаційних об'єктів:

$$Z_{i\_etalon} = \underset{j=1}{\overset{n}{M}}(z_{ij}) = \frac{1}{n}\sum_{j=1}^{n} \beta_j z_{ij}.$$

Обов'язковою умовою використання вагових коефіцієнтів є їх нормування: $Z_{i\_etalon} = \underset{j=1}{\overset{n}{etalon}}(z_{ij})$. При великій розбіжності значень певних показників можливе використання логарифмічної шкали.

У якості іншої модифікації класичного таксонометричного методу пропонується використовувати різні способи пошуку еталону для різних показників (мінімум, максимум, зважене середнє тощо). Загальний вираз для еталону в такому разі записуємо у вигляді:

$$Z_{i\_etalon} = \underset{j=1}{\overset{n}{etalon}}(z_{ij}).$$

Після визначення еталону потрібно визначити віддаленість всіх об'єктів від еталону. Як міру віддаленості можна використовувати квадрат евклідової відстані у m-вимірному просторі показників, або евклідову відстань, або інші міри, що є традиційними для кластерного аналізу (міра Чебишова, Хемінга, ступенева відстань тощо). У класичному варіанті використовуємо квадрат евклідової відстані для обчислення R_j віддаленості повединки j-го обєкту від еталонної поведінки:

$$R_j = \sum_{i=1}^{m} (z_{ij} - Z_{i\_etalon})^2 \ ,$$

або з урахуванням коефіцієнтів ρ_i ваги показників:

$$R_j = \sum_{i=1}^{m} \rho_i (z_{ij} - Z_{i\_etalon})^2 \ .$$

Об'єкти з поведінкою, найближчою до еталонної, тобто з найменшими R_j, будуть вважатись найбільш безпечними. Найвіддаленіші найбільш небезпечними.

Додаткова аналітична інформація може бути отриманою з аналізу зміни у часі віддаленості об'єктів від еталону, з прогнозування збільшення рівня інформаційних небезпек та з визначення основних тенденцій.

Серед нових тенденцій можуть бути як збільшення або поява нових інформаційних небезпек, з одного боку, так і перехід ознак небезпек до категорії ознак безпеки, з іншого боку.

На рис. 3.38 наведені зміни параметрів для різних об'єктів спостереження. По горизонталі наведені номери параметрів, а по вертикалі - їх значення. Товста лінія відповідає еталону (в цьому випадку за критерієм максимуму).

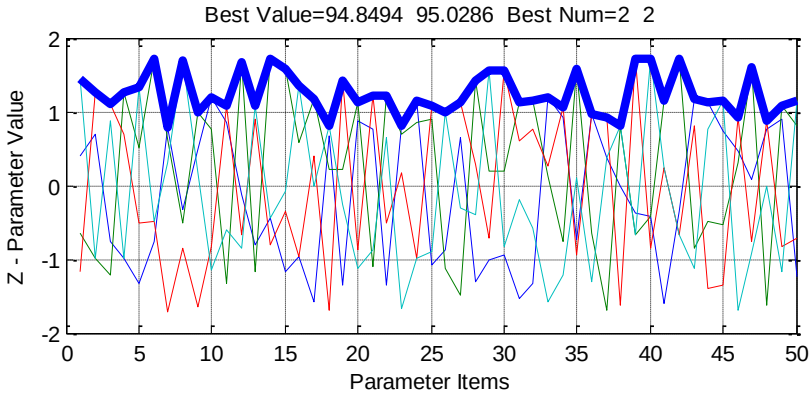


Рис. 3.38. Поточні значення параметрів для набору об'єктів та параметри еталонного об'єкту (мажоранта)

На рис. 3.39 наведена дендрограма, в якій по горизонталі розташовані номери об'єктів спостереження, а по вертикалі їх евклідова відстань від еталону в просторі показників.

Об'єкти з найменшими відстанями є найбільш безпечними. Є певні групи об'єктів, віддалених від еталону, але їх багато, і за тривалим спостереженням їх можна об'єднати в кластер нетипових, але безпечних об'єктів. Хоча також можливо, що це буде кластер підготовки масованої атаки. Конкретний тип кластеру визначається за сукупністю ознак і аналізом конкретної ситуації. Але одне є незаперечним – ці об'єкти потребуватимуть особливої уваги. Найбільш підозрілими завжди є одиночні об'єкти в зоні великих відстаней. У нашому разі – це об'єкти за номерами 12, 17, 31.

Моделювання в системі MATLAB показало, що реалізація запропонованого алгоритму на звичайній бюджетній обчислювальній

техніці є можливою. Так, час розрахунків для 4000 об'єктів спостереження за 50 параметрами склав 2.136149 секунди, без врахування часу на реалізацію графіки.

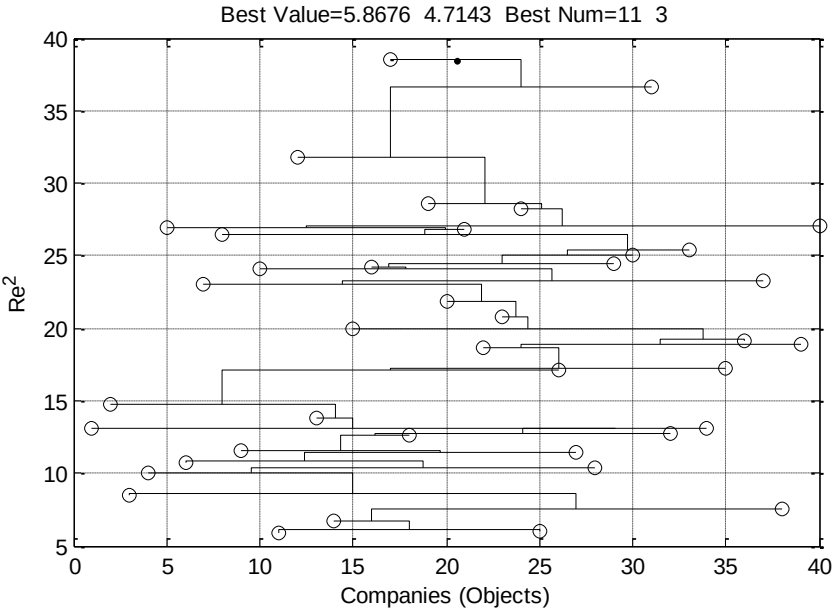


Рис. 3.39. Дендрограма об'єктів спостереження

Наведений вище підхід не є складним за своєю суттю і може бути легко реалізований відповідними програмними засобами. Але проблема полягає в тому, що кількість інформаційних об'єктів, які потрібно досліджувати, може бути досить великою. Тому наступним питанням є дослідження вимог та спроможності звичайних бюджетних комп'ютерів щодо реалізації запропонованого алгоритму.

ВИСНОВКИ

Проведений аналіз стану поширення і використання шкідливих програм свідчить, що кількість інцидентів інформаційної безпеки, зокрема вірусних атак, зростає темпами, які значно перевищують темпи розвитку інформаційних технологій. Найбільш небезпечними для інформаційних систем з мережевою складовою є загрози «нульового дня». Ці висновки обумовлюють актуальність даної роботи.

Зроблений огляд методів та засобів захисту від різних типів вірусів, зокрема тих, що впливають на виконання управлінських функцій, дозволяє запропонувати формування захищеного середовища інформаційного простору органу державного управління. В системі управління інформаційною безпекою визначено важливість застосування моделей прогнозування.

Визначено, що для відпрацювання засобів протидії загрозам корисним є використання досвіду боротьби з вірусами та інфекціями в медичній та біологічній галузях. Проведений аналіз показав аналогічність процесів розвитку біологічних епідемій та епідемій кібератак.

У цій роботі набув подальшого вдосконалення епідеміологічний підхід до моделювання розвитку кібератак за допомогою логістичних рівнянь з урахуванням латентного періоду розвитку атаки. Водночас уперше запропонований підхід щодо управління кібербезпекою під час епідемій шляхом вжиття своєчасних заходів щодо утримання стану інфраструктури на доепідеміологічному рівні.

Також набув подальшого вдосконалення таксонометричний метод протидії загрозам «нульового дня» шляхом виявлення об’єктів з нетиповою поведінкою. Адаптований в роботі таксонометричний метод дозволяє в автоматичному режимі виділяти потенційно небезпечні об’єкти мережі для їх відслідковування з метою організації вчасної протидії.

Показано, що точність моделі має відповідати точності вхідних даних та степені невизначеності щодо закономірностей процесу, який моделюється. При високій степені невизначеності та неточності вхідних даних більш доцільними є грубі моделі. Розглянуті базові моделі прогнозування, з яких найбільш адекватною для задач прогнозування розвитку інформаційної безпеки обрана логістична модель.

Модель, що запропонована, коректне прогнозує розвиток епідемії та дозволяє планувати правильні випереджувальні заходи. Корисною особливістю моделі є наочність всіх змінних та математичних перетворень, що дозволяє чітко відстежувати адекватність моделі та вчасно вносити необхідні корективи. Новим результатом є відокремлення даних щодо кількості об'єктів та об'єктів, які знаходяться в інкубаційному періоді, за часовими стадіями відповідних станів, що надає додаткові можливості для керування протиепідемічними заходами.

Введенні у моделі коефіцієнти K_S, K_E дозволили математично визначити різні види протиепідемічних заходів. Надалі ці параметри доцільно використовувати для контролювання динаміки розвитку кібератаки з метою обмеження її поширення на рівні, що не доходить до рівня епідемії (тобто стану, при якому відбувається повне блокування діяльності інформаційної системи).

Як показують результати подальшого моделювання, рівень епідемії залежить від другої необхідної умови, а час початку – від першої, що дозволяє декомпозувати означені умови під час чисельного експерименту щодо прогнозування можливих сценаріїв розвитку епідемій.

Додатковий виграш в часі та точності ідентифікації загроз можуть надати знання основних закономірностей розвитку кібератак.

Практична цінність отриманих результатів полягає у розробці конкретних алгоритмів та моделей, які можуть бути використані при побудові архітектури захищеного середовища функціонування веб-ресурсів органів управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Амелькин В.В. Дифференциальные уравнения в приложениях / Амелькин В.В. – М.: Наука. Гл.ред.физ.-мат. лит., 1987. – 160 с.

2. Аудит та управління інцидентами інформаційної безпеки: навч.посіб. / Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

3. Бароян О.В. Математика и епидемиология / Бароян О.В., Рвачев Л.А. – М.: Знание, 1977. – 63 с.

4. Бароян О.В. Моделирование и прогнозирование эпидемий гриппа для территории СССР / Бароян О.В., Рвачев Л.А., Иванников Ю.Г. – М.: ИЭМ. им. Н.Ф.Гамалеи, 1977. – 546 с.

5. Бірюков О. А. Концептуальні положення комплексної системи захисту інформації для веб-ресурсів органу державного управління / О. А. Бірюков, О. В. Нестеренко, І. Є. Нетесін, В. Б. Поліщук // Збірник матеріалів науково-практичного семінару «Методологічні питання інформатизації логістики в управлінні оборонними ресурсами». – УкрНЦ РІТ, ЦВСД Національного університету оборони імені Івана Черняховського (9 грудня 2016 р., м. Київ). – С. 58-62.

6. Боев Б.В. Гео-информационные системы и эпидемии гриппа / Б.В. Боев, В.В. Макаров // Ветеринарная патология. – 2004. – №3 (10). – С. 51-59. – [Електронний ресурс] Режим доступа: http://elibrary.ru/item.asp?id=9165685 (accessed 23 March 2017).

7. Боев Б.В. Гео-информационные системы и эпидемии гриппа / Б.В. Боев, В.В. Макаров // Вестник Российского университета дружбы народов. Серия: Сельськохозяйственные науки. Животноводство. – 2005. - №12. – С. 6-15.

8. Боев Б.В. Компьютерное моделирование в оценке последствий акта биологического терроризма / Б.В. Боев // Сб. докл. I Российского симпозиума по биологической безопасности. – М.: НИИ эпидемиологии и микробиологии им. Н.Ф. Гамалеи РАМН. – [Електронний ресурс] Режим доступа: www.bio.su. (accessed 23 March 2017)

9. Боев Б.В. Модель развития эпидемии гриппа a(h1n1) в России в сезон 2009 - 2010 годов / Б.В. Боев // Эпидемиология и вакцинопрофилактика. – 2010. – № 1. – С. 52-58.

10. Боев Б.В. Прогнозно-аналитические модели эпидемий (оценка последствий техногенных аварий и природних катастроф). Лекция в МФТИ для слушателей курса "Режим нераспространения и сокращения оружия массового поражения и национальная безопасность" / Б.В. Боев. – 2005. – 10 с. [Електронний ресурс] Режим доступа: http://www.armscontrol.ru/course/

11. Боев Б.В. Современный этап математического моделирования процессов развития и распространения инфекционных заболеваний / Б.В. Боев // Эпидемиологическая кибернетика: модели, информация, эксперименты. Сб. науч.тр. М., 1991. – С. 6-15.

12. Будько М.М. Вільне програмне забезпечення: український вибір / М.М. Будько, О.В. Нестеренко, І.Є. Нетесін. – К.: Альтерпрес, 2011. – 400 с.

13. Вентцель Е.С. Исследование операций / Е.С. Вентцель. – М.: Сов.радио, 1972. – 552 с.

14. Вьюн В. И. Об одном подходе к прогнозированию эпидемиологической обстановки по гриппу-ОРВИ с использованием временных рядов / В.И. Вьюн, Т.К. Еременко, Г.Е. Кузьменко, Ю. А. Михненко. // Математичні машини і системи. – 2011. – №2. – С.131-136.

15. География киберпреступлений. Западная Европа и Северная Америка / [Електронний ресурс] Режим доступа: https://securelist.ru/geografiya-kiberprestuplenij-zapadn/147/

16. Горбулін В.П. Системно-концептуальні засади стратегії національної безпеки України / В.П. Горбулін, А.Б. Качинський. – К.: ДП «НВЦ «Євро-атлантикінформ», 2007. – 592 с.

17. Гуд Г.Х. Системотехника. Введение в проектирование больших систем / Г.Х. Гуд, Р.Э. Макол; пер. с англ. – М.: Сов.радио, 1962. – 383 с.

18. Давыдов В.В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом / В.В. Давыдов // Зб. наук. праць «Системи обробки інформації». – Харків, 2012. – №3 (101). – Том 2. – С. 147-151.

19. Деева Э.Г. Грипп. На пороге пандемии: руководство для врачей / Э.Г. Деева. – М.: ГЭОТАР – Медиа. – 2008. – 208 с.

20. Добров Г.М. Прогнозирование науки и техники / Г.М. Добров. – М.: Наука, 1977. – 208 с.

21. Дослідження складних систем військового призначення / О.М.Загорка, С.П.Мосов, А.І.Сбитнев, П.І.Стужук. – К.: НАОУ, 2005. – 100 с.

22. Зайченко Ю.П. Основи проектування інтелектуальних систем: навч. посібн. / Ю.П. Зайченко. – К.: Видавничий дім "Слово", 2004. – 352 с.

23.История человечества – это история эпидемий // Сервер MedLinks.Ru. – 2012. – [Електронний ресурс] Режим доступу: http://www.medlinks.ru/article.php?sid=8650

24. Квейд Э. Анализ сложных систем / Э. Квейд; пер. с англ. под. ред. И.И.Ануреева, И.М.Верещагина. – М.: Сов. радио, 1969. – 520 с.

25. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста / К.Е. Климентьев. – М.: ДМК Пресс, 2013. – 656 с.

26. Колесник И. Екосистема. Эпидемия: Моделирование процессов распространения заболеваний / Ирина Колесник // Knol. – 12 июня 2010 года. – Version 40. – [Електронний ресурс] Режим доступу: http://knol.google.com/k/ирина-колесник/экосистема-эпидемия/16w02k60ur5gy/9

27. Кондратьев М. А. Методы прогнозирования и модели распространения заболеваний / М. А. Кондратьев // Компьютерные исследования и моделирование. – 2013. – Т. 5. – № 5. – С. 863–882.

28. Костюченко А. В. Киеве прошел Форум Cisco по сетевой безопасности, технологиям для совместной работы и ЦОД / А. В. Костюченко // Сайт новин Vido. – [Електронний ресурс] Режим доступу: http://vido.com.ua/article/13358/v-kiievie-proshiel-forum-cisco-po-sietievoi-biezopasnosti-tiekhnologhiiam-dlia-sovmiestnoi-raboty-i-tsod/

29. Моисеев Н.Н. Математические задачи системного анализа / Н.Н. Моисеев – М.: Наука, 1981. – 488 с.

30. Монахов Ю.М. Вредоносные програми в компьютерних сетях: учеб. пособие / Ю.М. Монахов, Л.М. Груздева, М.Ю. Монахов. – Владимирский гос.ун-т. – Владимир: изд-во Владим. Гос. Ун-та, 2010. – 72 с.

31. Науково-технічний звіт про науково-технічну роботу «Проведення передпроектних досліджень по забезпеченню інформаційної безпеки державного реєстру наукових установ, яким надається підтримка держави» / УкрНЦ РІТ, 2016. – 131 с.

32. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко. – К.: Наук. думка, 2009. – 352с.

33. Нестеренко О. В. Основи побудови автоматизованих інформаційно-аналітичних систем органів державної влади / О.В. Нестеренко. – К.: Наукова думка, 2005. – 628 с.

34. Нестеренко О.В. Застосування вільного/відкритого програмного забезпечення для підвищення рівня інформаційної безпеки комп'ютерних мереж органів державного управління / О.В. Нестеренко, І.Є. Нетесін, В.Б. Поліщук, Є.Б. Шушпанов // Матеріали науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» (17–20 листопада 2015 р., м. Київ). - Державний університет телекомунікацій Міністерства освіти і науки України. – Том IV «Сучасні технології інформаційної безпеки. – С. 53-55.

35. Нетесин И. Е. Модели безопасности и защиты в распределенных компьтерных середах / И. Е. Нетесин // Проблемы программирования. – 2000. – №3-4. – С. 148-158.

36. Отраслевой прогноз Аналитического центра InfoWatch в области информационной безопасности организаций в 2019 году // [Електронний ресурс] Режим доступу: https://www.infowatch.ru/index.php/analytics/digest/15204

37. Оуэн Д.Ф. Что такое экология? / Д.Ф. Оуэн; пер. с англ. – М.: Лесн.пром-сть, 1984. – 184 с.

38. Офіційни веб-сайт компанії Zillya! Вірусна енціклопедія // [Електронний ресурс] Режим доступу: https://zillya.ua/virus/all

39. Офіційний веб-сайт Міністерства охорони здоровья України. Травень 2012 р. // [Електронний ресурс] Режим доступу: http://www.moz.gov.ua/ua/portal/op_flu_100525_0.html

40. Поліщук В. Б. Програмне забезпечення: унікальне чи стандартне? / В. Б. Поліщук // ИТМ. Информационные технологии для менеджмента. – 2011. – №5. – С. 32-34.

41. Прайс Д. Малая наука, большая наука / Д. Прайс // Наука о науке: сб. статей; пер. с англ. – М.: Прогресс, 1966. – С. 281-384.

42. Пригожин И. Порядок из хаоса: Новый диалог человека с природой / И. Пригожин, И. Стенгерс. – М.: Прогресс, 1986. – 432 с.

43. Романенко Т.А. Діагностично-прогностичні критерії прогнозування тенденції розвитку епідеміологічного процесу кашлюку / Т.А. Романенко // Профілактична медицина, 2009. – №4(8). – С.17-23.

44. Саати Т.Л. Математические методы исследования операций / Т.Л. Саати. – М.: Воениздат, 1963. – 420 с.

45. Семенов В.М. Руководство по инфекционным болезням / В.М. Семенов, Т.И. Дмитраченко, В.М. Козин [и др.]; под. ред. В.М. Семенова. – М.: ООО «Медицинское информационное агентство», 2009. – 752 с.

46. Сильвестров А.Н. Многократно адаптивные системы идентификации / А.Н. Сильвестров, О.М. Папченко. – К.: Техніка, 1983. – 111 с.

47. Соловьйов С.О. Математичне моделювання і прогнозування захворюваності на ротавірусну інфекцію серед дітей до п'яти років в Україні / С. О. Соловьйов, І.О. Терещенко, І.В. Дзюблик // Медична інформатика та інженерія, 2012. – №1. – С. 23-29.

48. Управление киберрисками во взаимосвязанном мире. Основные результаты глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год. Январь 2015 // Офіційний сайт PricewaterhouseCoopers. [Електронний ресурс] Режим доступу: http://www.pwc.ru/ru/riskassurance/publications/assets/managing-cyberrisks.pdf

49. Уязвимости корпоративных информационных систем // [Електронний ресурс] Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/ corporate-vulnerabilities-2018/

50. Шевченко А.В. Грубі моделі розвитку в медицині / А.В. Шевченко, В.Л. Шевченко // Медична інформатика та інженерія, 2010. – №4. – С. 52-55.

51. Шевченко А.В. Математична модель прогнозування динамики епідемій / А.В. Шевченко, А.Л. Гепко // Профілактична медицина, 2011. – №3(15). – С. 3-6.

52. Шевченко А.В. Ретроспективний аналіз шляхів подолання глобальної екологічної кризи / А.В. Шевченко, В.Ю. Громенко // Зб.наук.праць ЦВСД НАОУ. – 2009. – №2(40). – С. 106-114.

53. Шевченко В.Л. Оптимізаційне моделювання в стратегічному плануванні / В.Л. Шевченко. – К.: ЦВСД НУОУ, 2011. – 283с.

54. Bartlett M.S. Some evolutionary stochastic processes / M.S. Bartlett // Journal of the Royal Statistical Society. – B11. – P. 211-229.

55. Bernoulli D. Essai d'une nouvelle analyse de la mortalite causee par la petite verole et des avantages de l'inoculation pour la prevenir / D. Bernoulli. – Mem. Math. Phys. Acad. Roy. Sci., Paris (1760). – P. 1-45.

56. Boev B.V. The computer program and mathematical model for the operative analysis and prognosis of outbreaks the hospital klebsiella infection among newborns / B.V. Boev, V.M. Bondarenko, C.P. Valencia // Medical Microbiology Letters. 1996. – T. 5. – № 1.

57. Bolot J. Cyber Insurance as an Incentive for Internet Security / J. Bolot, M. Lelarge // In Workshop in Economics of Information Security (WEIS) Seventh Workshop on Economics of Invormation Security, June, 2008. – P. 25–28.

58. Britton T. Stochastic epidemic models: survey / T. Britton. Cornell University. – Arxiv.0910.4443v1 [math.PR]. – P.1-26.

59. Britton T. Graphs with specified degree distribution, simple epidemics and local vaccination strategies / T. Britton, S. Janson and A. Martin-Lf // Adv. Appl. Prob. – 39. – P. 922-948.

60. Cohen F. Computer Viruses / F. Cohen. PhD thesis. – University of Southern California.

61. Cohen F. Computer Viruses: Theory and Experiment / F. Cohen // Computer and Security, 1987. – Vol.6. – №1. – P. 22-35.

62. Ducasse S. Software architecture reconstruction: a process-oriented taxonomy / S. Ducasse and D. Pollet // IEEE Transactions on Software Engineering, 2009. – №35(4). – P. 573–591.

63. ESET антивирус – официальный сайт Есет в Украине // [Електронний ресурс] Режим доступу: https://eset.ua/ru/ for_business/ endpoint_security

64. Euler L. Recherches generals sur la mortalite et la multiplication du genre humain / L. Euler. – Memoires de l'academie des sciences de Berlin, 1767. – P.144-164.

65. Farr W. Progress of epidemics / W. Farr // 2-nd Report of the regist. General of England and Wales, London, 1840.

66. Garetto M. Modeling Malware Spreading Dynamics / M. Garetto, W. Gong and D. Towsley // IEEE INFOCOM 2003. [Електронний ресурс] Режим доступу: www.ieee-infocom.org/2003/papers/46_01.pdf.

67. Geiger D. Managing the crowd: towards a taxonomy of crowdsourcing processes / D. Geiger, T. Schulze, S. Seedorf, R.C. Nickerson and M. Schader // In Proceedings of the 17th Americas Conference on Information Systems (Sambamurthy V and Tanniru M, Eds), AIS, Detroit, MI. [Електронний ресурс] Режим доступу:

https://pdfs.semanticscholar.org/ bb30/7fb8140d42e1a21c872eabfc9e400cf3347b.pdf.

68. Hasan H. A taxonomy of modes of knowledge sharing between disparate group / H. Hasan // In Proceedings of the 13th Pacific Asia Conference on Information Systems (Bapna R and Sambamurthy V, Eds), AIS, Hyderabad. [Електронний ресурс] Режим доступу: https://pdfs.semanticscholar.org/04c9/7b30378b1ff0050cc003d212612847cd335e.pdf.

69. Healthcare cybersecurity challenges in an interconnected world / Key finding from The Global State of Information Security. Survey 2015. [Електронний ресурс] Режим доступу: http://www.pwc.ru/en/ riskassurance/ publications/assets/ healthcare.pdf.

70. Independent Tests of Anti-Virus Software / [Електронний ресурс] Режим доступу: https://www.av-comparatives.org/

71. Internet Security Threat Trends from the World's Largest Civilian Threat Research / [Електронний ресурс] Режим доступу: https://www.symantec.com/about/analyst

72. Kendall D.G. Deterministic and stochastic epidemics in closed populations / D.G. Kendall // Proc. Thirs Berkley Symp. Math. Statist. E Prob., 4. – P.149-165.

73. Kephart J.O. Directed-graph epidemiocal models of computer viruses / J.O. Kephart and S.R. Whites // Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. – P. 343-358.

74. Kermack W.O. A contribution to the mathematical theory of epidemics / W.O. Kermack and A.G. McKendrick // Proc. Roy. Soc. Lond. A. – 1927, 115. – P. 700-721.

75. Krug S. A preliminary taxonomy for software failure impact: categorizing the impact on enterprises when software fails / S. Krug, H. Campidelli and R.C. Nickerson // In Proceedings of the 18th Americas Conference on Information Systems (Jessup L and Valacich J, Eds), Seattle, Washington. [Електронний ресурс] Режим доступу: Google Scholar Available at https://pdfs.semanticscholar.org/ 7e13/cf2f1148b227fa465b22f984cf8f54e4c2e3.pdf.

76. Leveille J. Epidemic Spreading in Technological Networks / Jasmin Leveille. – 2002 September 3. 100p. [Електронний ресурс] Режим доступу: www.hpl.hp.com/techreports /2002/HPL-2002-287.pdf (доступ 23 березня 2017).

77. Lotka A. J. Relation Between Birth Rates and Death Rates / A. J. Lotka // Science, 26 (1907). – P. 21-22.

78. López T.S. Taxonomy, technology and applications of smart objects / T.S. López, D.C. Ranasinghe, B. Patkai and D. Mcfarlane // Information Systems Frontiers 11(4). – Pp. 1–20. [Електронний ресурс] Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.838.4246&rep=rep1&type=pdf.

79. Microsoft Security Intelligence Report VOLUME 23 // [Електронний ресурс] Режим доступу: http://info.microsoft.com/rs/157-GQE-382/images/EN-AU-CNTNT-eBook-Security-GDPR-Microsoft-SIR-Volume-23%5B1%5D.pdf

80. Moor D. Code-red: a case study on the spread and victims of an internet worm / David. Moor, Colleen. Shannon, J. Brown // In: Proceedings of the ACM SIGCOMM/USENIX Internet Measurement Workshop.

81. Moor D. The Spread of the Code-Red Worm (CRv2) / David Moor, Colleen Shannon. – Офицiйний сайт Центру прикладного аналiзу Інтернет даних CAIDA. [Електронний ресурс] Режим доступу: https://www.caida.org/research/security/code-red/coderedv2_analysis.xml

82. Nandakumar Sri M. Numerical Methods / Sri M. Nandakumar. – VI semestr. Core Course. B Sc Mathematics. – Univ. of Calicut. School of Distance Education. – 2011. – 223 p.

83. Nickerson R. Taxonomy development in information systems: a literature survey and problem statement / R. Nickerson, J. Muntermann and U. Varshney // In Proceedings of the 16th Americas Conference on Information Systems (Santana M, Luftman JN and Vinze AS, Eds), AIS, Lima. [Електронний ресурс] Режим доступу: Google Scholar Available at https://pdfs.semanticscholar.org/f75d/d219dde068353678c69877fb5dfd7db12 c95.

84. Nickerson R. A Method for Taxonomy Development and Its Application in Information Systems / R. Nickerson, J. Muntermann and U. Varshney // Europ. Journ. of Information Systems. May 2013, Vol.22, Issue 3. – Pp. 336–359. [Електронний ресурс] Режим доступу: https://doi.org/10.1057/ejis.2012.26.

85. Nickerson R. Taxonomy development in information systems: developing a taxonomy of mobile applications / R. Nickerson, U. Varshney, J. Muntermann and H. Isaac // In Proceedings of the European Conference on Information Systems (Newell A, Whitley EA, Pouloudi N, Wareham J and Mathiassen L, Eds), AIS, Verona. [Електронний ресурс] Режим доступу: Google Scholar Available at https://halshs.archives-ouvertes.fr/file/index/ docid/375103/filename/ ECIS_2009_taxonomy_final_3.pdf.

86. Netesin I. Expernet - An intelligent multi-agent system for WAN management / I. Netesin, I. Vlahavas, N. Bassilliades, I. Sakellarion, M. Molina, S. Ossowski, I. Futó, Z. Pásztor, J. Szeredi, I. Velbitskiyi, S. Yershov // IEEE Intelligent Systems, 2002. – № 1, vol 17. – P. 62-72.

87. Onwubuoya C. Numerical Simulation of a Computer Virus Transmission Model using Euler Corrector Method / C. Onwubuoya, S. T. Akinyemi, O.I. Odabi and G.N. Odachi // International Digital Organisation for Scientific Research IDOSR Journal of Applied Sciences, 2018. – 3(1). – P. 16-28.

88. Onwubuoya C. An Approximate Solution of a Computer Virus Model with Antivirus using Modified Differential Transform Method / C. Onwubuoya, D.E. Nwanze, J.S. Erejuwa, S.T. Akinyemi // International Journal of Engineering Research (IJERT). – Vol.7, Issue 04, April-2018. – Pp.154-161. [Електронний ресурс] Режим доступу: www.ijert.org

89. Pratama. Computer Worm Classification / Pratama, Andhika, Rafrastara, Adi Fauzi // International Journal of Computer Science and Information Security. – 10. P.21-24.

90. Ross R. The prevention of malaria / R. Ross. – 2-nd ed., London: John Murray, 2011.

91. Scale-free_network // Wikipedia. [Електронний ресурс] Режим доступу: https://en.wikipedia.org/wiki/Scale-free_network

92. Serazzi G. Computer Virus Propagation Models / G. Serazzi, S. Zanero. – In: Calzarossa M.C., Gelenbe E. (eds) Performance Tools and Applications to Networked Systems. MASCOTS 2003. Lecture Notes in Computer Science, vol 2965. Springer, Berlin, Heidelberg. – Pp.26-50. [Електронний ресурс] Режим доступу: https://doi.org/10.1007/978-3-540-24663-3_2

93. Shalaeva O.A. Taksonometrichesky method rejtingovoj ocenki dejateljnosti razlichnykh tipov i form seljskokhozjajstvennykh organizacij [Taksonmetric Method of Rating Evaluation of Different Types and Forms of Agricultural Organizations] / O.A. Shalaeva, V.I. Kolesnev // Problems of the economy (Belarusian State Agricultural Academy), 2011. – C .237-244. [Електронний ресурс] Режим доступу: https://cyberleninka.ru/article/n/taksonometricheskiy -metod-reytingovoy-otsenki-deyatelnosti-razlichnyh-tipov-i-form-selskohozyaystvennyh-organizatsiy.

94. Shevchenko A. The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems / A. Shevchenko, V. Shevchenko // 2017 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Polyana, April 20-23, 2017. – Pp. 174-177. [Електронний ресурс] Режим доступу: http://ieeexplore.ieee.org/document/7937561/ DOI: 10.1109/MEMSTECH.2017.7937561.

95. Shevchenko A. The Epidemiological Approach to Prognosis and Management of Information Incidents / A. Shevchenko, J. Shcheblanin, V. Shevchenko // Наука і техніка Повітряних Сил Збройних Сил України, 2017. –№ 4 (29). – С. 145-150. [Електронний ресурс] Режим доступу: http://www.hups.mil.gov.ua/periodic-app/journal/nitps/2017/4

96. Staniford S. How to own the internet in your spare time / S. Staniford, V. Paxson, N. Weaver // Proceedings of the 11th USENIX Security Symposium (Security '02).

97. Stollenwerk N. Population Biology and Criticality. From Critical Bith-Death Processes to Self-Organized Criticality in Mutation Pathogen Syestem / Nivo Stollenwerk, Vincent Jansen. – London. – Imperial College Press. – 224 p.

98. The Global State of Information Security Survey 2016. Turnaround and transformation in cybersecurity // Офіційний сайт PricewaterhouseCoopers. [Електронний ресурс] Режим доступу: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

99. The Global State of Information Security Survey 2017. Turnaround and transformation in cybersecurity // Офіційний сайт PricewaterhouseCoopers. [Електронний ресурс] Режим доступу: https://www.pwc.com/gx/en/ issues/cyber-security/information-security-survey.html.

100. The Global State of Information Security Survey 2018. Turnaround and transformation in cybersecurity // Офіційний сайт PricewaterhouseCoopers. [Електронний ресурс] Режим доступу: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

101. Umbreen F. Numerical Modeling of Susceptible Latent Breaking-out Quarantine Computer Virus Epidemic Dynamic / Fatima Umbreen, Ali Mubasher, Ahmed Nauman and Rafiq Malik Muhammad // Heliyon. – 4 (2018) e00631. – P. 1-21.

102. Van Doorn E.A. Quasi-stationary distribution and convergence to quasi-stationary of birth-death processes / E.A. Van Doorn // Adv. Appl. Prob. – 23. – P. 683-700.

103. Yang L.-X. The impact of patch forwading on the prevalence of computer virus: A theoretical assessment approach / L.-X. Yang, X. Yang, Y. Wu //Applied Mathematical Modelling, 2017. – Vol. 43. – P. 110-125.

104. Yao Y. An Epidemic Model of Computer Worms with Time Delay and Variable Infection Rate / Yu Yao, Qiang Fu, Wei Yang, Ying Wang, Chuan Sheng // Hindawi. Security and Communication Networks. - Vol.2018, Art.ID 9756982. – P.1-11. [Електронний ресурс] Режим доступу: https://doi.org/10.1155/2018/9756982.

105. Zhang C.. Global Behavior of a Computer Virus Propagation Model on Multilayer Networks / Chunming Zhang // Hindawi. Security and Communication Networks. – Vol. 2018, Art.ID 2153195. – P.1-9.

[Електронний ресурс] Режим доступу: https://doi.org/10.1155/2018/2153195.

106. Zhang Z. Dynamics of a Computer Virus Propagation Model with Delays and Graded Infection Rate / Zizhen Zhang, Limin Song // Hindawi. Advances in Mathematical Physics. Vol.2017, Article ID 4514935, p.1-13. [Електронний ресурс] Режим доступу: https://doi.org/10.1155/2017/4514935

Наукове видання

Шевченко Віктор Леонідович
Нестеренко Олександр Васильович
Нетесін Ігор Євгенійович
Шевченко Аліна Віталіївна

ПРОГНОЗНЕ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ ВІРУСНИХ ЕПІДЕМІЙ

За редакцією В.Б. Поліщука

Літературний редактор
Беляченко А. В.

Підп. до друку 10.12.2019 Формат 60Х84/16
Папір офіс. Гарнітура Times New Roman. Друк. офс.
Ум. друк. арк. 8,66. Обл.-вид. арк. 5,35.
Наклад 300 прим. Зам. 164

Український науковий центр розвитку інформаційних технологій
(УкрНЦ РІТ)
Свідоцтво ДК № 6628
03127, м. Київ, пр. Глушкова, 44.
тел. 500-90-95
www.itdev.rit.org.ua, info@rit.org.ua

Віддруковано згідно з наданим оригінал-макетом
ТОВ «ПроФормат»
Україна, 04080, м. Київ, вул. Кирилівська, 86
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
Серія ДК № 5942 від 11.01.2018 р