© Kononovich V., Kononovich I., Kopytin Yu., Staikutsa S. Influence of delays decision action for information protection on information security risks // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 83-91.

ВПЛИВ ЗАТРИМКИ ПРИЙНЯТТЯ ЗАХОДІВ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ НА РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Володимир Кононович[1], Ірина Кононович[2], Юрій Копитін[3], Сергій Стайкуца[1]

[1]*Одеська національна академія зв'язку ім. О.С. Попова, Україна*
[2]*Одеська національна академія харчових технологій, Україна*
[3]*КП «Обласний інформаційно-аналітичний центр», Україна*

КОНОНОВИЧ Володимир Григорович, к.т.н.

Рік та місце народження: 1941 рік, с. Баришівка, Київської обл., Україна.
Освіта: Одеський електротехнічний інститут зв'язку, 1968 рік.
Посада: доцент кафедри інформаційної безпеки та передачі даних з 2010 року.
Наукові інтереси: теорія інформації, неокібернетика та кібербезпека.
Публікації: більше 200 наукових публікацій, навчальні посібники та авторські свідоцтва.
E-mail: kononovich@mail.ru

КОНОНОВИЧ Ірина Володимирівна

Рік та місце народження: 1979 рік, м. Одеса, Україна.
Освіта: Одеська державна академія холоду, 2001 рік.
Посада: викладач кафедри інформаційних технологій та кібербезпеки Одеської національної академії харчових технологій з 2002 року; аспірант ОНАХ.
Наукові інтереси: теорія інформаційного виробництва, інформаційна безпека.
Публікації: 27 наукових статей та доповідей на міжнародних конференціях і семінарах.
E-mail: kononovich@mail.ru

КОПИТІН Юрій Вікторович

Рік та місце народження: 1989 рік, м. Одеса, Україна.
Освіта: Одеська національна академія зв'язку, 2011 рік.
Посада: т.в.о. начальника відділу забезпечення захисту інформації КП «Обласний інформаційно-аналітичний центр» з 2013 року. Аспірант ОНАЗ
Наукові інтереси: управління інформаційною безпекою, економічна безпека.
Публікації: 16 наукових статей та доповідей на міжнародних конференціях і семінарах, навчальний посібник.
E-mail: ykopytin@odessa.gov.ua

СТАЙКУЦА Сергій Володимирович, к.філос.н.

Рік та місце народження: 1978 рік, м. Вознесенськ, Миколаївської обл., Україна.
Освіта: Одеська національна академія зв'язку, 2001 рік.
Посада: доцент кафедри інформаційної безпеки та передачі даних з 2010 року.
Наукові інтереси: соціальна філософія, інформаційна безпека, системи захисту бізнесу.
Публікації: 18 наукових робіт, серед яких монографія, навчальні посібники, наукові статті та доповіді на міжнародних конференціях і семінарах.
E-mail: s.staikuca@gmail.com

Анотація. *У статті проведено аналіз основних причин виникнення затримки у вжитті заходів із захисту інформації. Визначено, що існуючі моделі оцінки ризиків в переважній більшості базуються на статистичних підходах, орієнтуються на статичні моделі і слабо враховують динамічний характер взаємодій у кіберпросторі. Відомий інструментарій не дає можливості враховувати для аналізу та оцінки ризиків затримки у вжитті заходів захисту. Розроблено модель динаміки ризиків інформаційної безпеки внаслідок дії атаки, яка реалізовується протягом певного інтервалу часу через одну й ту саму вразливість,*

та модель впливу затримки прийняття рішень із захисту інформації на динаміку ризиків інформаційної безпеки. Розроблені моделі дають можливість створювати більш гнучкі засоби оцінювання та розраховувати відносну величину ризику інформаційної безпеки як на основі статистичних даних, так і на якісних оцінках, зроблених за допомогою нелінійних моделей із запізнюванням. Результатами проведеного моделювання показано, що своєчасне прийняття заходів і засобів протидії загрозам дозволить знизити ризики інформаційної безпеки.

Ключові слова: *захист інформації, ризики інформаційної безпеки, загрози, вразливість, атака, кіберзлочинність, нелінійна динаміка, модель систем із запізнюванням.*

Вступ

За даними Міжнародного Союзу Електрозв'язку зростання кіберзлочинності має експоненціальний характер [1]. Так, за даними ресурсу Zone-H [2] за 2012 рік відбулось 1 192 326 успішно реалізованих несанкціонованих дій щодо інформації веб-сайтів, за результатами дослідження Ponemon and AccessData [3] 86% компаній не встигають вчасно відстежити кіберзлочинців та за даними компанії McAffee [4] кількість примірників шкідливого програмного забезпечення у кіберпросторі перевищила 172 млн. примірників. Однією з причин такої ситуації є стрімке зростання різноманітності й складності характеру загроз та їх джерел, збільшення кількості вразливостей елементів сучасного кіберпростору. При цьому, існуючі засоби та заходи захисту не здатні в повному обсязі протидіяти зазначеній множині загроз. Згідно із законом У. Росс Ешбі щодо необхідного різноманіття: «Кількість регулювання має бути не меншою різноманіття збурень, проти якого направлене регулювання [5, 6]». Складність поведінки системи протидії повинна перевищувати складність поведінки атакуючої системи. Звідси випливає й висловлювання Є.А. Касперського щодо «важливості складних технологій (безпеки) в епоху складних атак [7]». Системи безпеки стають складними. Загальною проблемою є вдосконалення та підвищення ефективності систем забезпечення інформаційної безпеки з урахуванням ризиків безпеки сучасного кіберпростору. Для побудови ефективних комплексних систем захисту інформації в інформаційно-телекомунікаційних системах необхідно проводити аналіз, моделювання та оцінку ризиків.

Аналіз існуючих досліджень

Для багатьох організацій захищеність комп'ютерної мережі стає одним із найважливіших пріоритетів, при цьому системи безпеки стають все складнішими. З іншого боку, у багатьох сферах, які характеризуються підвищеною складністю, спостерігаються процеси інтеграції, конвергенції й уніфікації, які стимулюються застосуванням і розповсюдженням інформаційних технологій. Інтегральний підхід «до множини різних ризиків» безпеки декларується в [6]. Однією з головних причин ризиків інформаційної безпеки є «людський фактор» і, зокрема, запізнювання в прийнятті нагальних рішень щодо застосування заходів і засобів захисту. Запізнювання виникає як технологічне, соціальне, так і психологічне явище. За час одного покоління людей змінюють одна одну декілька нових технологій, які непередбачено виявилися надто вразливими. Потрібен час для вироблення протидії. Як соціальне явище запізнювання виникає, наприклад, за необхідності навчання користувачів, фахівців та осіб, що приймають рішення. Люди, особливо старшого віку, можуть мати труднощі з перенавчанням і сприйманням нових загроз. Як психологічне явище запізнювання виникає внаслідок звикання до технологій і недооцінки ризиків. Запізнювання прийняття рішень щодо захисту інформації стало одним із важливих проблем безпеки. Вплив запізнювання прийняття заходів захисту інформації на ризики інформаційної безпеки як науковцями, так і практиками досліджено недостатньо.

Для дослідження ризиків інформаційної безпеки зручно використовувати моделі динамічних систем, під якими сьогодні розуміють системи будь-якої природи (фізичну, хімічну, біологічну, соціальну, економічну, інформаційну тощо), стан якої змінюється, дискретно або неперервне у часі. Активно розвиваються методи динамічного моделювання процесів розповсюдження вірусів, червів, та протікання інших видів загроз. Застосовується математичний апарат, який розроблено давно для вивчення моделей розповсюдження інфекційних хвороб, біологічних та інших об'єктів. Вперше в російськомовній технічній літературі огляд цих методів наведено у [8], де стверджується, що «аналіз класичних моделей епідемій ... підходять для вивчення комп'ютерних інфекцій навіть дещо краще, ніж для біологічних об'єктів». Огляд сучасного стану аналітичних моделей розповсюдження червів зроблено СПИИРАН [9], а спроба врахувати запізнювання із введення в дію антивірусів за допомогою ймовірнісних методів викладена у [10]. Питання оцінки впливу запізнень заходів з протидії мережевим хробакам досліджено в [11]. Існуючі оцінки ризиків у переважній більшості базуються на статистичних підходах, орієнтуються на статичні моделі і слабо враховують динамічний характер взаємодій у кіберпросторі. Відомий інструментарій не дає можливості враховувати для аналізу та оцінки ризиків затримки у прийнятті рішень щодо заходів захисту інформації.

Метою роботи є дослідження впливу запізнювання у прийнятті рішень із захисту інформації на ризики інформаційної безпеки за допомогою логістичного рівняння та рівняння Хатчинсона.

I. Основна частина дослідження

В цілому сучасний кіберпростір представляє собою складну динамічну систему, що характеризується постійною конкурентною боротьбою порушників (кіберзлочинців, представників «сірого» бізнесу, крадіїв тощо) та захисників (дослідників систем безпеки, тестувальників, розробників програмного забезпечення, системних інтеграторів тощо), які здійснюють постійне всебічне дослідження та пошук нових загроз і вразливостей телекомунікаційних мереж, комп'ютерних систем, програмних застосувань і ресурсів. Перші, створюють засоби для нанесення атак, другі, розробляють виправлення для програмного забезпечення, створюють нові засоби захисту. Як відомо, побудова моделі загроз та виявлення вразливості елементу кіберпростору шляхом аналізу є результат творчої діяльності дослідника, який володіє певними навичками та знаннями. Слід зазначити, що порушник завжди перебуває в позиційній перевазі над стороною, що захищається, оскільки він зосереджує зусилля на певному об’єкті інформаційної діяльності або інформаційно-телекомунікаційній системі, а захисники повинні аналізувати та захищатися від усього вектору загроз. При цьому зазначені дії можуть бути прийняті зловмисниками без значних витрат та ризиків.

Спрощено процеси виявлення та усунення вразливості характеризується виникненням наступних двоїстих ситуацій: процес виявлення вразливості (відомості надано розробнику програмного забезпечення для усунення або ними користується виключно порушник), процес виправлення недоліків у програмному забезпеченні (недолік виправлено або не виправлено), процес встановлення оновлень кінцевими користувачами (оновлення встановлено або не встановлено) тощо. Всі ці процеси потребують певного часу на їх виконання, що й складає основу формування затримок у прийняті рішень із захисту інформації. На рис. 1 наведено приклад життєвого циклу шкідливого програмного забезпечення [12]. На рис. 1 наведені наступні умовні позначення: A-day – розроблення шкідливого програмного забезпечення; 0-day – поява шкідливого програмного забезпечення у кіберпросторі; D-day – перше виявлення шкідливого програмного забезпечення у кіберпросторі; R-day – протидія шкідливому програмному забезпечення (встановлення оновлення)

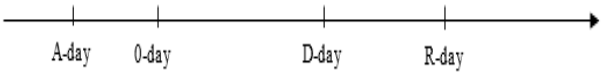


Рис.1. Життєвий цикл шкідливого програмного забезпечення

Основні причини, які приводять до затримки у прийнятті рішень із захисту інформації такі:

- більшість керівників вважає, що забезпечення інформаційної безпеки виключно технічна проблема, яка вирішується за допомогою технічних засобів, і не бажають виділяти кошти на утримання служби захисту інформації, навчання співробітників тощо;

- не всі співробітники організації розуміють необхідність виконання заходів та засобів захисту;

- поточна структура Інтернет будувалась за принципами прозорості та відкритості, а не безпечності;

- під час проектування інформаційно-телекомунікаційних систем вимоги із забезпечення інформаційної безпеки не приймають до уваги, а подальше впровадження захисних механізмів може бути складним та витратним;

- оцінити ризики програмного забезпечення із закритим кодом може лише його розробник. Всі інші можуть здійснити тестування програмного забезпечення методами сірої та/або чорної скриньки, однак це не дозволяє гарантувати відсутність недекларованих можливостей та вразливостей;

- недостатній рівень співробітництва між державою та приватним сектором, що майже унеможливлює отримання статистичної інформації про інциденти безпеки та започаткування централізованого банку даних, яким можна скористатися під час створення системи забезпечення інформаційної безпеки (СЗІБ) тощо.

Все це призводить до небажаних наслідків від вдалих атак зловмисників на активи організацій, заподіяння матеріального збитку та моральної шкоди користувачам, збільшення репутаційних втрат. Саме тому, дослідження процесів затримки у прийнятті рішень із захисту інформації та впливу затримок на ризики інформаційної безпеки набуває не абиякої ваги.

II. Модель затримки прийняття рішень із захисту інформації

Прийняття управлінських рішень щодо СЗІБ, як правило, здійснюється із затримкою (запізнюванням). В зв’язку з чим, СЗІБ відноситься до систем із запізнюванням, у яких результат впливу виявляється не відразу, а через певний час τ – час запізнювання. В економічних, біологічних, технічних та інших науках для подібних явищ широко використовуються моделі, які описуються рівняннями із запізнюванням. Рівнянням із запізнюванням прийнято називати рівнянням відносно невідомої функції $x(t)$, що пов’язує швидкість зміни функції $x(t)$ з її значеннями в поточний момент часу t та певний момент часу $t-\tau$, де постійна $\tau > 0$ [13].

Розглянемо вплив запізнювання з прийняття рішень щодо захисту інформації на ризик інформаційної безпеки за допомогою найпростіших моделей, а саме логістичного рівняння та рівняння Хатчинсона.

У загальному випадку ризик R виражають у вигляді поєднання наслідків події (включаючи зміни в обставинах) і пов'язаної з нею можливістю її виникнення [14, 15], та розраховують за виразом, який можна представити наступним чином:

$$R = F \cdot D = \frac{N}{N_A} D' \quad (1)$$

де F – річна частота події, інакше кажучи ймовірність виникнення збитків;

D – очікуваний одиничний збиток (величина збитку від однієї успішної атаки);

N – кількість успішно реалізованих атак протягом року;

N_A – загальна кількість атак, що виникають протягом року.

Розрахунку зазначених параметрів присвячено різні методики, однак питання впливу запізнювання у прийнятті заходів на ризик у них розкрито недостатньо. Під час проведення оцінки впливу запізнень будемо враховувати наступне:

- під ризиком інформаційної безпеки будемо розуміти ймовірність того, що певна загроза буде експлуатувати вразливість активу або групи активів і тим самим нанесе шкоду організації [16];

- вважатимемо, що ризику піддаються типові активи, для яких характерні типові наслідки, тобто очікуваний одиничний збиток у різні моменти часу є константою;

- для демонстрації динаміки росту негативних наслідків від небезпечних атак на інформаційно-телекомунікаційну систему скористаємось логістичним рівнянням Ферхюльста [17]

$$N' = r(1 - \frac{N}{N_c})N, \quad (2)$$

значення змінних і параметрів якого, в інтерпретації з питань інформаційної безпеки, автори роботи пропонують прийняти наступним чином:

N' – похідна від N, яка описує швидкість реалізації вдалих атак; N – потенційна кількість вдалих реалізацій загрози щодо активу; N_c – середня кількість активів, схильних до дії загрози; r – коефіцієнт легкості реалізації певної загрози через певну вразливість.

Дискретним аналогом логістичного закону є логістичне відображення, яке було застосоване біологом Р. Меєм для аналізу конкретної біологічної ситуації,

$$N_{n+1} = r(1 - N_n)N_n, \quad (3)$$

де $N_1, N_2, ..., N_n,$ – можуть відповідати чисельності або біомасі різноманітних видів [18].

Швидкість реалізації вдалих атак пропорційна потенційній кількості вдалих реалізацій загрози та коефіцієнту легкості реалізації певної загрози через певну вразливість і представлена виразом:

$$N' = rN. \quad (4)$$

У відсутності перешкод кількість атак (кіберзлочинів) зростає за експоненціальним законом

$$N(t) = e^{rt} N_0, \quad (5)$$

де N_0 – кількість кіберзлочинів у початковий момент часу.

Вираз у дужках із рівняння (2) враховує обмеження на розповсюдження загроз (кількість активів, схильних до дії загрози). Потенціалом для зростання кількості атак є наявність активів, які мають вразливість, необхідну для успішної реалізації загрози. Кількість вдалих атак із плином часу виходить на постійне значення, асимптотично наближаючись до середнього значення N_c. За фізичним сенсом розглядаємо лише додатні розв'язки. Розв'язок диференціального рівняння (2), знайдений чисельним методом за початкових умов $N(0) = 1$ (є один актив, щодо якого здійснено вдалу атаку), показано на рис. 2.

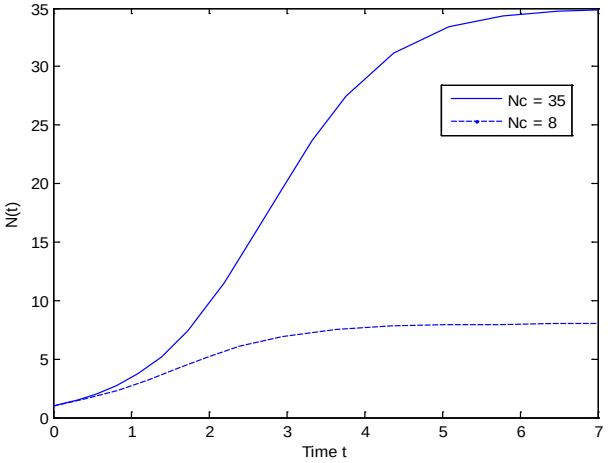


Рис.2. Характерні графіки зростання кількості атак, що описуються логістичним законом

Коли у комп'ютерній мережі є, наприклад 35 активів, що піддаються впливу загрози, то зростання кількості однотипних атак описує крива, яка зображена суцільною лінією. Якщо в мережі прийнято заходи та засоби, які повністю перекривають вразливість активу і тим самим роблять процес реалізації загрози неможливим, тобто залишилось, наприклад, лише 8 незахищених активів, то зростання кількості однотипних атак описується кривою, яка зображена пунктиром. Час на графіках продемонстровано в умовних одиницях. Зауважимо, що логістична крива, яка зображена пунктиром, буде відповідати дійсності, якщо засоби та заходи захисту впроваджуються миттєво, як тільки но буде виявлено відповідну вразливість.

Динаміка рівняння (2) характеризується трьома різними етапами:

початковим, коли порушник діє невпевнено та повільно реалізовує атаку через певну вразливість (умовний інтервал від 0 до 0.5);

активним, коли порушник набирає впевненість у собі і реалізовує атаки з максимальною швидкістю (умовний інтервал від 0.5 до 6);

насищення, коли порушник починає боятися, що буде виявлений (умовний інтервал від 6 до 7).

Підтвердимо адекватність моделі шляхом аналізу її основних властивостей, для чого проінтегруємо (2), використовуючи метод розподілу змінних.

$$N(t,N_0)=\frac{N_c}{1+(\frac{N_c}{N_0}-1)e^{-rt}},t\geq 0. \qquad (6)$$

Властивості рішень рівняння:

1) при $N_0>0$ маємо $N(t,N_0)>0, t\geq 0$;

2) $\lim\limits_{t\to+\infty} N(t,N_0)=K$;

3) при $0<N_0<K$ функція $N(t,N_0)$ зростає, а при $N_0>K$ спадає;

4) положення рівноваги $N(t)\equiv K, t\geq 0$, глобально асимптотично стійке.

Із зазначених властивостей видно, що у випадку не прийняття заходів та засобів протидії загрозі всі активи рано чи пізно будуть піддані дії атаки. Окрім цього, чим вище коефіцієнт легкості реалізації певної загрози через певну вразливість r, тим скоріше будуть активи піддані атаці.

Зазначимо, що дотепер звести число вразливостей до нуля на практиці не вдається, оскільки жоден засіб та захід захисту не може гарантувати відсутність недоліків: проектування (неповнота або неточність проведеного аналізу процесів інформаційної діяльності), розроблення (неякісність інженерних, програмних та апаратних засобів захисту або документації на систему забезпечення ІБ), впровадження (помилки інсталяції та конфігурування засобів захисту, недостатнє навчання користувачів) та використання механізмів безпеки (повне або часткове невиконання заходів захисту, неправильне або неналежне використання засобів захисту).

Отже, логістичний закон описує динаміку росту вдалих атак, коли нема заходів та засобів протидії загрозі та не враховує всі аспекти боротьби з використанням механізмів безпеки, зокрема, запізнювання.

На практиці прийняття заходів та засобів захисту від дії загроз проводять з певним запізнюванням. Причинами запізнювання можуть бути об'єктивні та суб'єктивні фактори. Для моделювання СЗІБ із запізнюванням використаємо рівняння, яке запропонував у 1948 р. Г. Хатчинсон:

$$N'(t)=r(1-\frac{N(t-\tau)}{K})N(t), \qquad (7)$$

де τ – час запізнювання.

Найпростішим дискретним аналогом рівняння Хатчинсона [11] є рівняння

$$N_{n+1}=r(1-N_{n-1})N_n. \qquad (8)$$

Рівняння (7), (8) відрізняються від рівнянь (2), (3) тим, що в них введено додатну постійну τ – час запізнювання, яка враховує фактор запізнювання з прийняття заходів та засобів щодо протидії загрозі.

Рівняння (7) описує наступний процес: кількість вдалих атак зростає в однорідному середовищі – у комп'ютерній мережі з однаковими (типовими) комп'ютерами. Мається задана кількість поживної речовини – вразливостей активів, які приводять до реалізації загрози. Кількість поживної речовини поновлюється з числа невразливих активів внаслідок впровадження засобів та заходів захисту. Приклад графіку чисельного розв'язку рівняння (7) показано на рис. 3 для двох випадків $\tau=1.3$, $\tau=2$ (час в умовних одиницях).

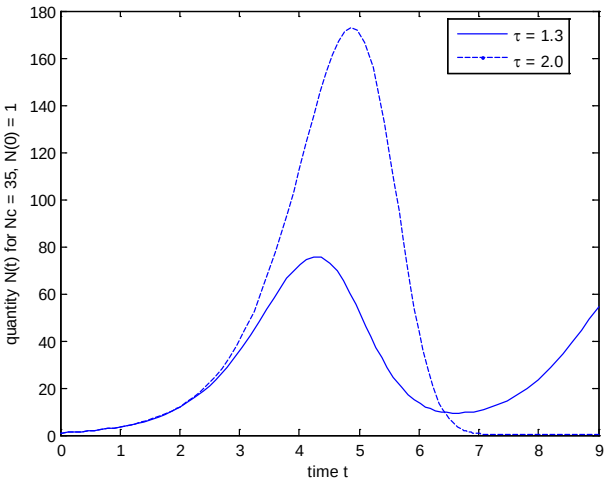


Рис.3. Характерний графік зростання кількості атак при запізнюванні з прийняттям заходів та засобів захисту

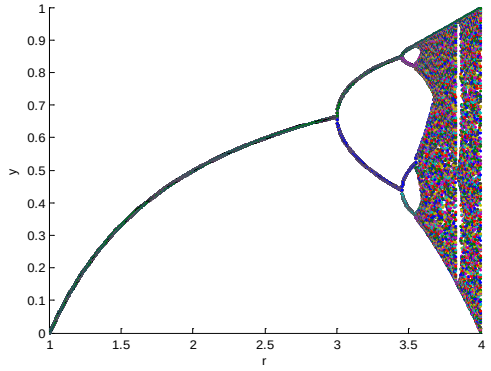
Розв'язок диференційного рівняння з запізнюванням отримано за допомогою програми, розробленої у середовищі Matlab, витяг з лістингу якої виглядає так:

```
global R1 K1 tau1
R1 = 1.28; K1 = 35; tau1 = 1.3; N0 = 1.001; N00 = 1;
options = ddeset('Events',@events,'InitialY',N0,...
'RelTol',1e-4,'AbsTol',1e-7);
sol = dde23(@ddes,tau1,N00,[0, 9],options);
plot(sol.x, sol.y)
% ------------------------------
function dydt = ddes(t,y,Z)
 dydt = R1*y*(1 - Z/K1);
end
```

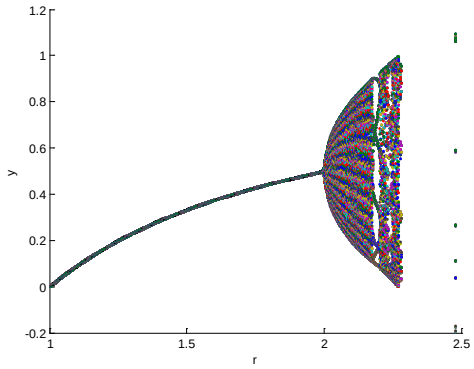
Введення додатної постійної τ – це спроба врахувати фактор запізнювання. Рівняння (7) описує наступну ситуацію: «вид заселений у однорідному середовищі, міграційні фактори не суттєві, мається задана кількість їжі, яка відновлюється при зменшенні численності популяції», [6] (див. ; гл.9, § 1.1, формула (3)). Ситуація з атакою описується в цій моделі наступним чином: загроза розповсюджується у комп'ютерній мережі з типовими елементами, є задана кількість активів, які схильні до дії загроз.

Рішення рівняння (7) має періодичний коливальний характер за певного набору параметрів. Із графіків видно, що запізнювання приводить до коливального процесу. Період коливань більший за час запізнювання. Зі збільшенням τ – часу запізнювання збільшується амплітуда і період коливань. У техніці таке явище називають «перерегулюванням». Коливальний характер зростання кількості атак пояснюється наступним. За малої кількості реалізованих атак та відсутності заходів і засобів захисту йде активне зростання кількості реалізованих загроз. Через деякий час, із запізнюванням, починають використовувати заходи і засоби захисту. Це приводить до зменшення «плодовитості» загроз - зменшується коефіцієнт вразливості. Але для меншої кількості загроз ресурсів може вистачати, тоді їх кількість знову починає зростати. Це може бути із-за того, що не на всіх комп'ютерах в мережі встановлено засоби захисту, або вони функціонують некоректно. Виникає повторна

хвиля атак. Процес має коливальний характер. Аналіз показує, що інтенсивність коливань зростає при збільшенні коефіцієнта вразливості та часу запізнювання τ .



a) біфуркації логістичного рівняння



b) біфуркації рівняння Хатчинсона

Рис.4. Модель настання динамічного хаосу в дискретних відображеннях (2) і (8)

Райтом [6] було доведено, що рівняння (4) лінійно стійке при

$$r\tau < \frac{\pi}{2} \tag{9}$$

і дає розв'язок у вигляді коливань навколо стану N_c . При $\tau = 0$ рівняння (8) перетворюється у логістичне рівняння (2). Незважаючи на свою простоту рівняння Ферхюльста та Хатчинсона можуть демонструвати складну поведінку і детермінований хаос. При великих значеннях часу запізнювання можуть виникати біфуркації, сингулярності, втрата стабільності. На рис. 4 показані біфуркаційні дерева цих рівнянь.

Класичне біфуркаційне дерево логістичного рівняння (2) на рис. 4.a має біфуркації подвоєння періоду по Файгенбауму. При збільшенні параметру r – коефіцієнта легкості реалізації певної загрози через певну вразливість, спостерігається перша біфуркація. Режим монотонного зростання або згасання коливань змінюється на режим згасаючих коливань. При подальшому збільшенні коефіцієнта r кількість біфуркацій збільшується і за $r > 3{,}6$ наступає хаос.

Біфуркаційне дерево рівняння із запізнюванням (8) на рис. 4.b більш складне. Мають місце біфуркації подвоєння періоду, а хаотичні коливання спостерігаються вже після першої біфуркації. При $r > 2{,}3$ спостерігаються сингулярності, тобто обчислення переривається при досягненні машинної нескінченності.

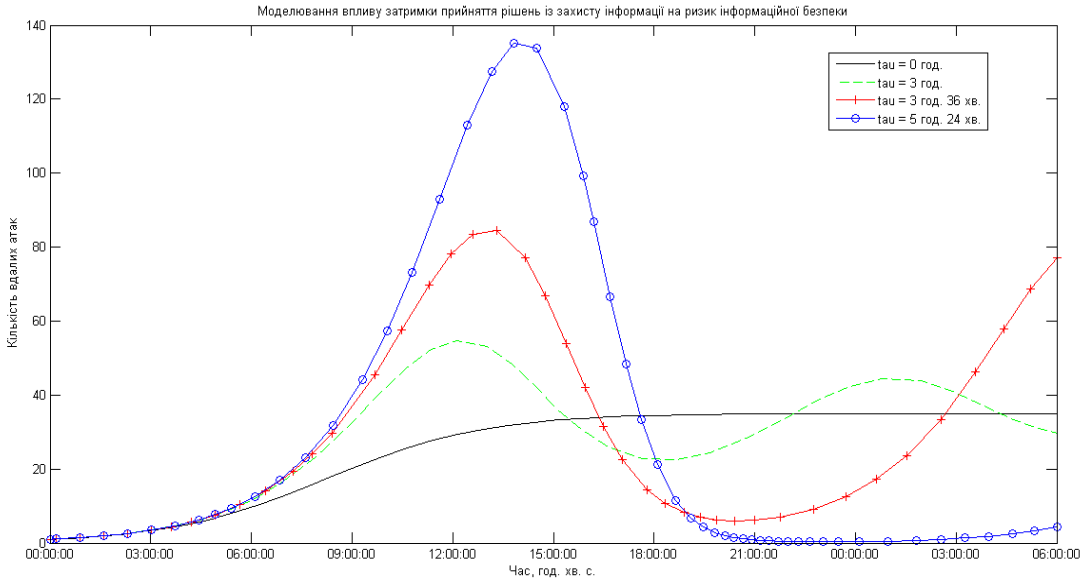


Рис. 5. Моделювання впливу затримки прийняття рішень із захисту інформації на ризик інформаційної безпеки

III. Вплив затримки прийняття рішень із захисту інформації на ризики інформаційної безпеки

Маючи розв'язок рівняння (7) легко перейти до обчислення ризику. Покажемо це за допомогою спрощеного рівняння (8). Нагадаємо, що одиночний збиток ми вважаємо константою, тобто незалежним від інтервалу спостереження. Тоді, знаходимо величину N із (1) і підставляємо у (8). Отримуємо

$$R_{n+1} = r\left(1 - \frac{N_A}{D} R_{n-1}\right) R_n \tag{10}$$

На рис. 5 представлено модель, яка наочно демонструє безпосередню залежність між затримкою у прийняті рішень із захисту інформації та ризиком інформаційної безпеки, а саме, чим більше затримка у прийняті рішень із захисту інформації, тим стрімкіше зростає ризик інформаційної безпеки. Для оцінки впливу запізнювання рішень на величину ризику проведено чисельне моделювання і знайдені відносні величини

$$rr = \frac{R(\tau)}{R(\tau = 0)}, \qquad (11)$$

які показують у скільки разів збільшується ризик при запізнюванні.

У табл. 1 наведені результати моделювання, де rr_{max} – максимальна величина відносного ризику rr_c – середня величина відносного ризику.

Для наочності отримані результати представлено на рис. 6.

Верхня крива на цьому рисунку відноситься до максимальних величин відносного ризику, нижня – до середніх величин відносного ризику

Таблиця 1

Оцінки залежності відносного ризику від величини запізнювання у прийнятті рішень

Запізнювання, τ	Максимальна величина відносного ризику, rr_{max}	Середня величина відносного ризику, rr_c
3 год.	1,57	1,08
3 год. 36 хв.	2,41	1,25
5 год. 24 хв.	3,86	1,97
6 год.	4,93	2,39

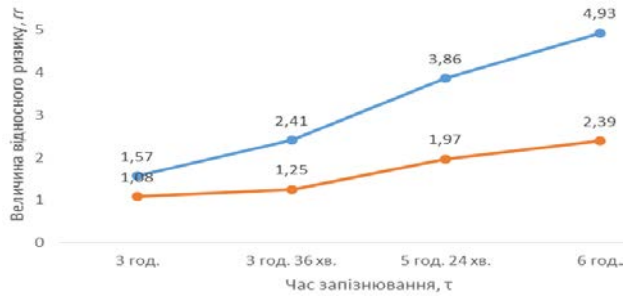


Рис. 6. Залежність величини відносного ризику *rr* від часу запізнювання τ

Адекватність використання рівняння Хатчинсона у питаннях забезпечення інформаційної безпеки підтверджується наступним:

- чим менше величина вразливості r, тим довше відбувається реалізація атаки на активи організації (при цьому графік стає менш похилим);
- чим більше час затримки τ, тим більш негативні наслідки настануть для організації у випадку, якщо порушник буде використовувати одну і ту саму вразливість для реалізації загрози;
- чим більше час затримки τ, тим більше ймовірність виникнення коливань (біфуркацій), оскільки представники служби захисту інформації не будуть знати з чого починати протидію, може розпочатися хаос.

На відміну від моделі Ферхюльста, зазначена модель враховує інерцію в реакції на атаки порушників, коливальний характер наближення кількості інцидентів безпеки до стаціонарного значення, можливість стійкого функціонування обмеженої кількості комп'ютерів у мережі.

Раніше прийнято було вважати, що мале запізнювання слабко впливає на поведінку системи. Інтуїтивне уявлення про те, що чим більше запізнювання, тим більше його дестабілізуючий ефект, не зовсім правильне. У СЗІБ навіть малий час запізнювання є небезпечним, оскільки швидкість розповсюдження небезпечних команд мережею Інтернет менше 1 с.

У запропонованої моделі є наступні недоліки:

- не враховується, що захищений від певного типу загрози комп'ютер більше не піддається її впливу (у випадку закриття вразливості), або загроза модифікується і проти неї немає заходів захисту, тоді процес починається спочатку;
- модель оперує кількісними даними, для отримання яких ще треба розробити методику та потужну систему чисельного моделювання з урахуванням більшого числа чинників.

Але результати моделювання, які проведені в цій роботі свідчать, що запізнювання з прийняттям рішень щодо захисту інформації та в інших ситуаціях управління приводить до збільшення ризиків втрат або збитків. Звернемо увагу на те, що збільшення ризиків проявляється двічі. Перший раз збитки виникають, коли число інцидентів з інформаційною безпекою збільшується, а захист запізнюється. По друге, збитки виникають коли кількість інцидентів падає, а витрати на захист ще залишаються занадто високими.

Окрім цього, зловмисники «розмножуються» швидше при відсутності контролю та покарання за неправомочні дії. Відсутність контролю та безвідповідальність провокує людей на аморальну поведінку. І навпаки, кількість зловмисників зменшується в умовах контрольованості й справедливості.

Висновки

Розроблено модель динаміки ризиків інформаційної безпеки внаслідок дії атаки, яка реалізовується протягом певного інтервалу часу через одну й ту саму вразливість, та модель впливу затримки прийняття рішень із захисту інформації на динаміку ризиків інформаційної безпеки, яка враховує величину вразливості, обсяг активів, що піддаються дії загрози, та час запізнювання прийняття заходів і засобів захисту. Розроблені моделі дають можливість створювати більш гнучкі засоби оцінювання та розраховувати відносну величину ризику інформаційної безпеки як на основі статистичних даних, так і на якісних оцінках, зроблених за допомогою нелінійних моделей із запізнюванням. Результатами проведеного моделювання показано, що своєчасне прийняття заходів і засобів протидії загрозам дозволить знизити ризики інформаційної безпеки та уникнути хаотичних процесів. Отримані результати

дозволяють підвищити ефективність роботи систем захисту інформації та формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем оцінки ризику.

Література

[1] Марко Обисо. Развитие международного сотрудничества в области кибербезопасности. Глобальный ответ на глобальный вызов / Marco Obiso, Cebersecuritycoordinator, ITU, Switzerland // Межрегиональный семинар для стран Европы, Азиатско-Тихоокеанского содружества независимых государств (Європа-АТР-СНГ) «Современные методы борьбы с киберпреступностью». — Одеса, Украина, 28-30 марта 2012.

[2] Zone-H. Unrestricted information. — Режим доступа: http://www.zone-h.org/

[3] McAfee Threats Report: Third Quarter 2013. — Режим доступа: http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf

[4] Смирнов Евгений. Большинство компаний не справляется с реакцией на кибератаки. — Режим доступа: http://securityb2b.cnews.ru/news/top/index.shtml?2014/03/03/562921

[5] Эшби У.Р. Введение в кибернетику / У. Р. Эшби; [Пер. с англ. Д.Г. Ламути. Под ред. В.А. Успенского]. — М. : Изд-во «Иностр. лит.», 1959. — 432 с.

[6] Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. — М.: РАН, 2000. — 249 с. — Режим доступа: http://risk.keldysh.ru/risk/risk.htm

[7] Отчет «Лаборатории Касперского»: Java под ударом – эволюция эксплойтов в 2012-2013 гг. — 26 с. — Режим доступа: http://www.securelist.com/ru/analysis/208050816/Otchet_Laboratorii_Kasperskogo_Java_pod_udarom_evolyutsiya_eksploytov_v_2012_2013_gg

[8] Захарченко А.А. Черводинамика: причины и следствия / А.А. Захарченко // Защита информации. Конфидент. — № 2, 2004. — С. 50–55.

[9] Котенко И.В. Аналитические модели распространения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. Вып. 4. — СПб.: Наука. 2007. — С. 208-224. — Режим доступа: http://www.proceedings.spiiras.nw.ru/data/src/2007/04/00/spyproc-2007-04-00-15.pdf

[10] Гусаров А.Н. Модель запаздывания действия антивирусов при распространении в сетях комп'ютерных угроз / А.Н. Гусаров, Д.О. Жуков // Известия ОрелГТУ. Серия «Информационные системы и технологии». — 2008. — № 1-2/269(544). — С. 67-72.

[11] Yang Xiang. Propagation of Active Worms: A Survey / Yang Xiang, Xiang Fan, Wen Tao Zhu // The Journal of Supercomputing archive. — Vol. 51 Issue 2, February 2010. — P. 167-200

[12] Paul Vixie Malware Repository Requirements. Policy Analysis / Paul Vixie, David Dagon. - Режим доступа: http://blog.washingtonpost.com/securityfix/DC-14-Vixie.pdf

[13] Тарасевич Ю.Ю. Избранные вопросы математического моделирования и численных методов. — Режим доступа: http://window.edu.ru/resource/936/38936/files/aspu03.pdf

[14] ISO Guide 73:2009. Risk management — Vocabulary. — Женева, 2013. — С. 15.

[15] Конеев И.Р. Информационная безопасность предприятия/ И.Р. Конеев, А.В. Беляев. — СПб. : БХВ-Петербург, Проспект, 2003. — 160 с.

[16] ISO/IEC 27005:2011. Information technology — Security techniques. — Information security risk management. — Женева, 2013. — С. 68.

[17] Долгий Ю.Ф. Математические модели динамических систем с запаздыванием: учеб. пос. / Ю.Ф. Долгий, П.Г. Сурков. — Екатеринбург : Изд-во Урал ун-та. 2012. — 122 с.

[18] Малинецкий Г.Г. Математические основы синергетики. Хаос, структура, вычислительный експеримент. — М. : КомКнига, 2005. — 312 с.

УДК 003.26:004.056.55 (045)

Кононович В.Г., Кононович И.В., Копытин Ю.В., Стайкуца С.В. Влияние запаздывания принятия мер по защите информации на риски информационной безопасности

Аннотация. *В статье проведен анализ основных причин возникновения задержки в принятии мер по защите информации. Определено, что существующие модели оценки рисков в подавляющем большинстве основаны на статистических подходах, ориентируются на статические модели и слабо учитывают динамический характер взаимодействий в киберпространстве. Известный инструментарий не позволяет учитывать для анализа и оценки рисков задержки в принятии мер защиты. Разработана модель динамики рисков информационной безопасности в результате действия атаки, реализуемой в течение определенного интервала времени через одну и ту же уязвимость, и модель влияния задержки принятия решений по защите информации на динамику рисков информационной безопасности. Разработанные модели позволяют создавать более гибкие средства оценивания и рассчитывать относительную величину риска информационной безопасности, как на основе статистических данных, так и на качественных оценках, выполненных с помощью нелинейных моделей с запаздыванием. Результатами проведенного моделирования показано, что своевременное принятие мер и средств противодействия угрозам позволит снизить риски информационной безопасности*

Ключевые слова: *защита информации, риски информационной безопасности, угрозы, уязвимости, атаки, киберпреступность, нелинейная динамика, модель систем с запаздыванием.*

Kononovich V., Kononovich I., Kopytin Yu., Staikutsa S. Influence of delays decision action for information protection on information security risks

Abstract. *The article analyzes the main causes of delay in taking measures to protect the information. Determined that the existing models of risk assessment overwhelmingly is based on statistical approaches, guided by static models and doesn't take into account the dynamic nature of interactions in cyberspace. Known tool doesn't allow to use delay in taking protective measures in process of risk analysis and assessment. Proposed a model of the dynamics of information security risks as a result of the attack, implemented within a specified time interval through the same vulnerability, and a model of the impact of delay in decisions on the protection of information on the dynamics of information security risks. The developed models allow you to create more flexible tools of evaluating and calculating the relative value of information security risk both on the basis of statistical data and the qualitative assessments made by using nonlinear models with delay. The simulation results shows that timely introduction of measures and means to counter threats will reduce information security risks.*

Key words: *information security, information security risks, threats, vulnerabilities, attacks, cybercrime, nonlinear dynamics, model of systems with delay.*

Отримано *7 лютого 2014 року*, затверджено редколегією *26 лютого 2014 року*