УДК 004:004.65

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В СИСТЕМАХ N-КАНАЛЬНОГО ДІАЛОГОВОГО СПІЛКУВАННЯ

Мясіщев О.А., Джулій А.В., Джулій В.М., Чешун В.М.
Хмельницький національний університет

Досліджено проблеми організації захисту інформації систем n-канального діалогового спілкування. Запропоновано модель процесу оцінки захищеності інформації, імовірнісні функції станів процесу, основний показник надійності здійснюваного захисту інформації. Узагальнено отримані результати на випадок системи захисту n-канального діалогового спілкування.

Ключові слова: захист інформації, система захисту, функції станів, надійність, багатоканальне спілкування.

Постановка проблеми. Збільшення спроб несанкціонованого доступу нелегальних користувачів до інформації з електронних джерел потребує розробки та впровадження спеціалізованих систем захисту (СЗ) інформації.

Призначення СЗ – максимально повне виключення протиправних (контрафактних) вторгнень. Стосовно ж реально функціонуючих СЗ справедливо вести мову лише про певний ступінь нейтралізації атак і мінімізації числа можливих проникнень в інформаційну систему, яку захищають.

За таких умов природно ставити питання про дослідження дієвості виконуваного захисту та його надійність. Для вирішення подібних задач має бути розроблено інструментарій кількісної оцінки досліджуваних параметрів.

Аналіз останніх досліджень і публікацій. Проблема оцінки надійності СЗ в наявних наукових публікаціях раніше не обговорювалася, принаймні, на рівні змістовного кількісного аналізу, хоча вона є однією з ключових в комп'ютерних технологіях [1,2]. Основна причина цього – саме по собі таке оцінювання представляє задачу, вирішувану в ситуації ризику і невизначеності. Ризик виражається стохастичним характером атак на інформаційне поле об'єкта і, отже, недетермінованістю обчисленої оцінки [2]. Невизначеність задачі полягає в обмеженні спостережень[5]: СЗ здатна фіксувати тільки відбивані спроби нелегального проникнення; факти успішних (для нелегалів) проникнень, що відбулися, СЗ не реєструє. Проте і в цих умовах застосуванням відповідного математичного апарату можна її результативного рішення.

Стохастичне оцінювання можливостей діючої системи захисту на даному проміжку часу тривалістю t пов'язане перш за все з аналітичною побудовою моделі функціонування СЗ. Така модель дозволяє, в принципі, вирішити два важливих питання: здійснювати прогнозування ситуації на об'єкті, що захищається, по нелегальних вторгненнях в його інформаційне поле; приблизно оцінювати надійність СЗ при вказаній вище умові невизначеності.

Виділення не вирішених раніше частин проблеми. Постановка й проведення дослідження можливостей програмно – апаратних засобів захисту електронних джерел інформації являє собою актуальною дослідницькою задачею [1] і мають своєю метою розробку математичної моделі функціонування СЗ на розглянутому проміжку часу тривалістю t. При цьому теоретична модель повинна бути простою і за прийнятими статистичними критеріями адекватною спостережуваним випадкам відбивання атак нелегальних користувачів.

Стохастичне оцінювання можливостей діючої системи захисту на розглянутому проміжку часу тривалістю t зв'язано, насамперед, з аналітичною побудовою моделі функціонування СЗ. Модель дозволяє вирішити два питання:

– здійснювати прогнозування ситуації на об'єкті, що захищається, за нелегальними вторгненнями у його інформаційне поле;

– приблизно оцінювати надійність СЗ при відзначеній раніше умові невизначеності [2], обумовленій тим, що система захисту не здатна фіксувати фактинелегальних проникнень в інформаційне поле об'єкта, які відбулись.

Статистика відбивання атак нелегальних користувачів показує, що, із прийнятною для практики похибкою, імовірнісну модель функціонування СЗ можна побудувати у вигляді марківського однорідного за часом ланцюгового процесу зміни станів СЗ по числу невідбиваних нелегальних проникнень, розглядаючи систему захисту як найпростішу розімкнуту пуасонівську систему [3]. Не описуючи випадковий процес вичерпним чином, ця модель все-таки дає досить повне представлення про нього, оскільки дозволяє розрахувати на будь який момент часу t імовірність перебування СЗ у тому або іншому стані й здійснювати прогнозування ситуації на об'єкті, що захищається, по нелегальних вторгненнях у його інформаційне поле.

Вхідний у діалог із системою захисту потік випадкових атак (вторгнень) нелегалів будемо характеризувати постійною інтенсивністю λ – середнім числом атак в одиницю часу. СЗ, впливаючи на цей потік, ділить його на два потоки: відбиваних атак з інтенсивністю λ_0 й невідбиваних атак з інтенсивністю $\lambda_н$.

Між перерахованими потоками виконується [3] балансове рівняння

$$\lambda = \lambda_0 + \lambda_н, \qquad (1)$$

називане «рівнянням витрати». З (1) будемо мати

$$\frac{\lambda_0}{\lambda} + \frac{\lambda_н}{\lambda} = 1. \qquad (2)$$

Перше відношення в (2) позначимо через P_{OA}, друге – через P_{HA}.

Імовірність

$$P_{OA} = \frac{\lambda_0}{\lambda} \qquad (3)$$

є не що інше як імовірність відбивання атак нелегальних користувачів діючої на об'єкті системи захисту (або імовірність припинення системою захисту спроб нелегального проникнення в інформаційне поле об'єкта).

Імовірність

$$P_{HA} = \frac{\lambda_н}{\lambda} \qquad (3^*)$$

є ймовірністю протилежної події й доповнює P_{OA} до одиниці, тобто $P_{HA} = 1 - P_{OA}$.

Рівність (2) – строга і, якщо параметри λ, λ_0 найпростішої пуасонівської СЗ відомі теоретично точно, то показником P_{OA} можна «в середньому» оцінити

ступінь захищеності об'єкта від несанкціонованих вторгнень. Зрозуміло, що подібна усереднена оцінка на практиці не є самодостатньою, оскільки найчастіше навіть одиночне проникнення нелегального користувача до джерела інформації протягом деякого кінцевого відрізка часу T може мати досить негативні (і катастрофічні) наслідки. Необхідне введення такого імовірнісного показника, пов'язаного із тривалістю роботи СЗ, за допомогою якого можна було б однозначно судити про несанкціоновані вторгнення, що відбуваються, у будь-який момент часу. Рішення цього питання об'єктивно пов'язане з розробкою стохастичної моделі функціонування СЗ по припиненню нелегальних проникнень.

Припустимо, що встановлена на об'єкті СЗ безперервної дії працює безвідмовно й без збоїв протягом тривалого часу до її планового оновлення.

Мета статті. Сформулюємо задачу дослідження в такий спосіб.

1. Вважаючи відомими параметри λ, λ_0 пуасонівської СЗ, побудувати диференціальну марківську модель процесу «відбивання-невідбивання» атак нелегальних користувачів у варіанті одноканального діалогу.

2. Знайти рівняння імовірнісних функцій станів процесу (станів СЗ) у часі й на множині цих функцій виділити основний показник надійності (дієвості) здійснюваного захисту інформації. Дослідити отримані імовірнісні функцій.

3. Розробити методику застосування основного показника надійності захисту в умовах невизначеності по параметру λ.

4. Узагальнити отримані результати на випадок СЗ n-канального діалогового спілкування з нелегальними користувачами.

5. Показати моделі пуасонівських СЗ, неоднорідних за часом, коли $\lambda = \lambda(t) \neq const$, $\lambda_0 = \lambda_0(t) \neq const$.

Основна частина. Складемо диференціальні рівняння процесу. Ці рівняння можуть бути отримані або безпосередньо перерахуванням подій і підрахунком елементарних імовірностей цих подій, або на підставі графа станів СЗ. На рис. 1 побудований граф, яким геометрично інтерпретується досліджуваний процес. На графі позначено: S_0 – стан процесу, при якому число невідбиваних атак дорівнює нулю; S_2, S_4, S_6 – стани процесу, у яких СЗ має на своєму рахунку одне, два, три й т.д. пропущені вторгнення; S_1, S_3, S_5 – стани процесу, що відповідають входженню в контакт нелегального користувача з СЗ; $p_i(t)$ – імовірність перебування СЗ у стані S_k, k=0, 1, 2, ... за час t, відлічуване від початку процесу; λ, λ_0, $\lambda_н$ – інтенсивності потоків атак нелегальних користувачів (умовні щільності ймовірностей переходів СЗ між станами S_k).

Відповідно до графа, система диференціальних рівнянь А.Н. Колмогорова імовірностей станів СЗ набуде вигляду:

$$\begin{cases} \frac{dp_0(t)}{dt} = -\lambda p_0(t) + \lambda_0 p_1(t) \\ \frac{dp_1(t)}{dt} = \lambda p_0(t) - \lambda p_1(t) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \frac{dp_{2k}(t)}{dt} = (\lambda - \lambda_0) p_{2k-1}(t) - \lambda p_{2k}(t) + \lambda_0 p_{2k+1}(t) \\ \frac{dp_{2k+1}(t)}{dt} = \lambda p_{2k}(t) - \lambda p_{2k+1}(t), \quad k = 1,2,... \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases} \quad (4)$$

Зауважимо, що граф на рис. 1 нетранзитивний [3] і тому процес, описуваний системою рівнянь (4), неергодичний і не володіє стаціонарним режимом.

Суть процесу, що протікає в СЗ, полягає в наступному. Якщо подія потоку вторгнень із інтенсивністю λ припинено діями СЗ, то атака припинена й по закінченні діалогу СЗ повертається зі стану S_{2k-1} з інтенсивністю λ_0 в попередній стан S_{2k-2}, k=1, 2, ... Якщо ж подія вхідного потоку не припинена СЗ, то по закінченні діалогу система захисту з інтенсивністю $\lambda_н = \lambda - \lambda_0$ віртуально переходить зі стану S_{2k-1} в наступний стан S_{2k}. Невідбивані атаки змінюють характеристичні стани СЗ, що у даній задачі виступає в ролі їх «накопичувача».

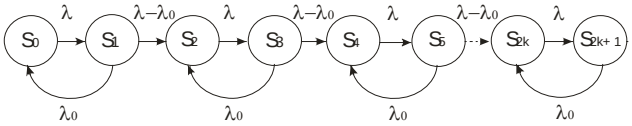

Рис. 1. Граф марківського процесу «відбивання – невідбивання» нелегальних вторгнень системою захисту інформаційного поля об'єкта

Джерело: розроблено авторами

Неергодичність процесу та накопичення даних не припинених вторгнень служить відмінною рисою розглянутої пуасонівської системи від відомих [3].

Імовірнісні функції (4) повністю розкривають можливості застосовуваної на об'єкті СЗ, виконуючи роль прогнозних рівнянь. На кожен наперед заданий момент часу значеннями цих функцій встановлюється розподіл числа невідбиваних незаконних проникнень в інформаційну систему. Імовірності (4) мають своїм призначенням рішення двох основних питань: прогнозування ситуації на об'єкті по очікуваних нелегальних проникненнях та оцінку дієвості (ефективності) застосовуваної програмно-апаратної СЗ у динаміці процесу.

Будь-яке порушення конфіденційності збереженої інформації нелегальними користувачами може мати досить серйозні негативні наслідки. Тому на множині ймовірностей $\{P_m(t)\}$ – основним функціональним показником надійності (ефективності) захисту рекомендується прийняти ймовірність

$$P_0(t) = \frac{1}{2}\left[\left(1 + \sqrt{\frac{\lambda}{\lambda_0}}\right)e^{-\left(\lambda - \sqrt{\lambda\lambda_0}\right)t} + \left(1 - \sqrt{\frac{\lambda}{\lambda_0}}\right)e^{-\left(\lambda + \sqrt{\lambda\lambda_0}\right)t}\right] \quad (5)$$

Значеннями показника (5) на розглянутому інтервалі часу (0, t), наприклад, в інтервалі календарного місяця, вичерпно характеризується повне припинення спроб нелегального доступу до інформації, що захищається, коли на рахунку використовуваної СЗ із параметрами λ, λ_0 немає жодного незаконного проникнення в інформаційну систему, також значеннями цього показника на розглянутому інтервалі (0, t) кількісно оцінюється ефективність системи захисту й виноситься оцінка доцільності її використання.

На додаток до показника $P_0(t)$ при більш глибокому дослідженні СЗ можна знаходити й інші оцінки – антитезу $\bar{P}_0(t) = 1 - P_0(t)$, якою виражається ймовірність не менш одного нелегального проникнення в інформаційне поле об'єкта; ймовірності $P_m(t)$, m>0 [2]. Це дає можливість побудувати *табличний розподіл таких вторгнень у часі* й знайти функцію математичного очікування зазначених подій $m(t)$, обумовлену формулою

$$m(t) = \frac{\lambda - \lambda_0}{2\lambda_0}\left[\sum_{k=1}^{\infty}\left(t\lambda_0 - 2k + 1\right)p_{2k-1}(t) + \lambda t \sum_{k=1}^{\infty} p_{2k-2}(t)\right], \quad (6)$$

де k=1,2, ..., ; $p_{2k-1}(t)$, $p_{2k-2}(t)$ – імовірності [2].

Безумовну зацікавленість представляє також такий показник як середня тривалість часу перебування процесу в парі станів $\{S_0, S_1\}$, або, що теж, середній час θ, протягом якого СЗ не допустить жодного нелегального доступу до інформації. Цей час обчислюється за формулою математичного очікування:

$$\theta = \int_0^{\infty} t d\bar{P}_0(t) = \int_0^{\infty} P_0(t) dt = \frac{1}{2}\left(1 + \sqrt{\frac{\lambda}{\lambda_0}}\right)\int_0^{\infty} e^{-\left(\lambda - \sqrt{\lambda\lambda_0}\right)t} dt + \frac{1}{2}\left(1 - \sqrt{\frac{\lambda}{\lambda_0}}\right)\int_0^{\infty} e^{-\left(\lambda + \sqrt{\lambda\lambda_0}\right)t} dt$$

Остаточно отримуємо:

$$\theta = \frac{2}{\lambda - \lambda_0} \quad (7)$$

Показник θ з (7) є індикатором, яким регламентується оптимальний термін дії комп'ютерної програми діалогу СЗ із користувачем за схемою «питання-відповідь». Після цього строку у всіх випадках бажане її оновлення.

Відзначимо, що для забезпечення схоронності інформації від нелегального доступу за інтенсивних атак, розроблювальні СЗ повинні мати високий ступінь надійності: $0.975 < P_{OA} < 1.0$. Забезпечення такого рівня надійності тільки програмно-апаратними засобами – непросте завдання. Тому, поряд із застосуванням цих засобів у всіх випадках, повинне бути передбачене регулярне (періодичне) відновлення основних структурних елементів використовуваної СЗ у сукупності із продуманою дезінформацією нелегальних користувачів.

Практичне застосування формул (1)-(6) прямо пов'язане із визначенням інтенсивності λ (параметр λ_0 відомий зі спостережень). Для визначення λ розроблена методика, де передбачені два варіанти оцінки надійності захисту:

1. Гарантованою розроблювачем імовірністю відбивання атак нелегальних користувачів P_{OA} за співвідношенням $\lambda = \frac{\lambda_0}{P_{OA}}$ з балансового рівняння [3].

2. Варіюванням параметра $\lambda > \lambda_0$ (за умови $0{,}75 \le \frac{\lambda_0}{\lambda} < 1$) і відшукання такого значення λ_{max}, при якому реалізується принцип найменших квадратів у формі $\sum(\lambda x - N_x)^2 \to \min$, де x – кількість діб, що минули від початку календарного місяця; N_x – кількість припинених спроб вторгнення на добу.

Імовірнісна модель (1)-(6) описує СЗ одноканального діалогового спілкування з нелегальними користувачами. Її узагальнення на випадок n-канальної пуасонівської системи не представляє принципових утруднень. Так, якщо по кожному з каналів інтенсивності λ, λ_0 зберігають постійне значення, то вираження основного функціонального показника надійності захисту інформації (нуль несанкціонованих проникнень) у цьому випадку буде таким:

$$P_0(t) = -\frac{(k_2 + n\lambda)}{k_1 - k_2}\left(1 + \frac{k_1 + n\lambda}{\lambda_0}\right)e^{k_1 t} + \frac{(k_1 + n\lambda)}{k_1 - k_2}\left(1 + \frac{k_2 + n\lambda}{\lambda_0}\right)e^{k_2 t}, \quad (8)$$

де k_1, k_2 – дійсні корені характеристичного рівняння $k^2 + (n+1)\lambda k + n\lambda(\lambda - \lambda_0) = 0$.

Висновки. Представлений формулами (1)-(6) процес функціонування СЗ не володіє ергодичною властивістю й стаціонарним режимом, а сама система захисту виступає в цьому процесі в ролі віртуального «накопичувача» не припинених нелегальних проникнень в інформаційне поле об'єкта. У цьому принципова відмінність розглянутої задачі від класичних пуасонівських схем. Аналогічні властивості узагальнення для n-канальної системи (8).

Список літератури:

1. Галицкий А.В Защита информации в сети – анализ технологий и синтез решений /А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньган – М.:ДМК Пресс, 2004. – 616 с.
2. Мясіщев О.А. Методика розрахунку показників надійності захисту ін-формації в умовах невизначеності / О.А. Мясіщев, А.В. Джулій // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2008. – № 2, – С. 143-148.
3. Эльсгольц Л.Э. Дифференциальные уравнения и вариационное исчисление / Л.Э. Эльсгольц – М.:«Наука», 1969. – 424 с.
4. Овчаров Л.А. Прикладные задачи теории массового обслуживания / Л.А. Овчаров М.:«Машиностроение», 1969. – 324 с.
5. Мясіщев О.А. Напрямки вирішення проблем захисту інформації в мережах. / О.А. Мясіщев, А.В. Джулій // Вісник ХНУ – 2009. – № 4, – С. 107-111.

Мясищев А.А., Джулий А.В., Джулий В.Н., Чешун В.Н.
Хмельницкий национальный университет

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В СИСТЕМАХ N-КАНАЛЬНОГО ДИАЛОГОВОГО ОБЩЕНИЯ

Аннотация
Исследованы проблемы организации защиты информации систем n-канального диалогового общения. Предложена модель процесса оценки защищенности информации, вероятностные функции состояний процесса, основной показатель надежности осуществляемой защиты информации. Обобщены полученные результаты на случай системы защиты n-канального диалогового общения.
Ключевые слова: защита информации, система защиты, функции состояний, надежность, многоканальное общение.

Myasischev A.A., Djuliy A.V., Djuliy V.N., Cheshun V.N.
Khmelnitsky National University

ESTIMATION OF INFORMATION SECURITY IN N-CHANNEL DIALOGUE COMMUNICATION SYSTEMS

Summary
Investigated the problems of organization information security systems with n-channels for dialogue communication. Proposed a model of information security evaluation process, the probability functions of the states of the process, also the main indicator of the information security reliability. Summarized the results obtained for the protection in case multi-channel communication system
Keywords: information security, security system, functions of the states, reliable, multi-channel communication.