УДК 004.056:323.1 **П.В. Хусаінов**

ПОКАЗНИК КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЛЯ ВИДІЛЕНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ

Стаття присвячена оприлюдненню деяких основних положень науково-практичного дослідження проблематики кібернетичної безпеки в сучасних комп'ютеризованих системах. Пропонується формальна постановка і модель показника кібернетичної безпеки на основі розгляду функціонування виділеної автоматизованої системи як випадкового процесу в умовах цілеспрямованих спроб непривілейованого авторизованого користувача-порушника розширити повноваження у межах сеансу роботи. Поняття виділеної автоматизованої системи (фізично відокремлена від мережевого середовища передачі з одинарним найпростішим потоком сеансів авторизованих користувачів) є одним з елементів авторської класифікації.

Ключові слова: кібернетична безпека, випадковий процес, ланцюг Маркова, розподіл Вейбулла, експонентний розподіл.

Вступ

На початку 90-х р. р. XX ст. теоретико-методологічний базис військового мистецтва збагатився новим напрямом досліджень шляхів здобуття переваги, перемоги над високотехнологічним противником застосовуючи узгоджені за місцем і часом сукупність методів, способів та прийомів інформаційно-психологічного впливу, погіршення якості і безпеки інформаційних процесів, більш оперативного збирання та аналізу розвідувальної інформації, радіоелектронного придушення, руйнування технічних засобів обміну даними і т. ін. [1-2].Невдовзі (початок 2000-х р.р.) тематика „інформаційних війн" (від англ. - informationandpsychologicalwarfare) почала активно обговорюватися в наукових колах нашої країни, але переважно у воєнно-прикладному аспекті її інформаційно-психологічної складової. Результат досить тривалого, так би мовити наївного періоду, за Д. Гільбертом, втілення у життя будь-якої нової теорії, призвів до появи організаційних структур з відповідними цілями, задачами і функціями, термінології щодо інформаційної безпеки держави у воєнній сфері [3]. Одночасно, разом з завершенням узгодження і прийняттям більш менш загальноприйнятого, консенсусного варіанту „термінологічних баталій", стала очевидною фактична відсутність суттєвих результатів щодо формалізації ключових понять які б дозволили перейти до строгих постановок задач аналізу і синтезу основних процесів інформаційно-технічної складової інформаційної боротьби. Так, оцінка ефективності системи захисту інформації (СЗІ) від загроз кібернетичного характеру потребують застосування тієї чи іншої строгої формальної постановки поняття „кібернетична безпека", який, в свою чергу, повинен бути органічно вплетений у чималий існуючий понятійний базис теорії і практики забезпечення безпеки інформації в автоматизованих системах (АС), максимально наближеним до практичних особливостей реалізації загроз так би мовити „кібернетичної" природи притаманних конкретним АС.

Аналіз останніх публікацій

Згідно [4] безпека інформації – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. Серед інших, одним з основних принципів побудови комплексів засобів захисту СЗІ є реалізація, у тому чи іншому вигляді, концепції диспетчера доступу сутність якої полягає у забезпеченні контролю всіх запитів суб'єктів (одиниць обчислювальної роботи) щодо використання об'єктів (файлів, каталогів, об'єктів пам'яті, пристроїв і т. ін.) з одночасним прийняттям рішення про допустимість чи заборону такого звертання згідно правил розмежування доступу (ПРД) як складової частини політики безпеки АС. Розмежування доступу в сучасних АС базується на застосуванні суб'єктно-об'єктної моделі. Вона надає розвинений формальний апарат для доведення суттєвих властивостей базових, ідеалізованих політик безпеки як дискреційної (від англ. - DiscretionaryAccessControl, DAC), так і мандатної (від англ. – MandatoryAccessControl, MAC) і, як наслідок, дозволяє застосовувати аксіому: безпека системи може бути цілком

забезпечена шляхом управління доступом суб'єктів до об'єктів протягом всього життєвого циклу АС [5]. При цьому практична реалізація того чи іншого варіанту політики безпеки обумовила необхідність впровадження органічного поєднання прав суб'єкта доступу як одиниці обчислювальної роботи породженої у контексті сеансу роботи користувача з певними повноваженнями (роллю) щодо використання об'єктів АС. Рольова політика безпеки (від англ. - RoleBaseAccessControl, RBAC) стала, у певному сенсі, компромісом між дискреційною і мандатною моделлю, а також основним підходом до організації розмежування доступу в сучасних операційних системах (ОС) загального призначення завдяки своїй практичній наочності і зрозумілості [6]. Так, успішна авторизація засобами ОС користувача, як фізичної особи, призводить до відкриття відповідного сеансу роботи та породження в його контексті первинного обчислювального процесу (лідер сеансу) з повноваженнями доступу до об'єктів згідно ролікористувача в АС. Запуск на виконання у межах сеансу роботи користувача інших програм призводить до формування у тому чи іншому вигляді ієрархічного дерева родинних відносин між створюваними обчислювальними процесами з наслідуванням повноважень лідера сеансу який виступає коренем дерева. Виходячи з викладеного, всі обчислювальні процеси або суб'єкти ініційовані користувачем мають однакові, співпадаючи з лідером сеансу повноваження щодо доступу до об'єктів АС у межах передбаченого для їх повноважень інформаційного домену [7]. Вважається, що у непривілейованого, звичайного користувача не має можливості розширити (змінити) свої повноваження, тим самим створити необхідні умови для виходу за межі свого інформаційного домену і порушення ПРД.

Сучасні ОС загального призначення реалізуючи концепцію примусової багатозадачності на основі розділення процесорного часу передбачають одночасне так би мовити „життя" значної кінцевої множини обчислювальних процесів. Деякі з них виконуються у контексті сеансів роботи звичайних, фізичних користувачів, але переважно більша частина це так звані службові обчислювальні процеси (демони) запущені у ході ініціалізації АС від імені так би мовити фізично неіснуючих користувачів як зручної абстракції первинної передачі повноважень (псевдокористувачі). Іншими словами в АС побудованої із застосуванням ОС загального призначення практично завжди, навіть коли здійснюється одиничний сеанс роботи фізичного користувача, є певна кількість обчислювальних процесів ініційованих від імені того чи іншого псевдокористувача з притаманним йому інформаційним доменом згідно виконуваних службових функцій, як правило, із застосуванням підвищених повноважень [8]. Відповідно примушення службового обчислювального процесу до виконання непередбаченої роботи у ході сеансу роботи фізичного користувача із набагато більшою імовірністю може призвести до певного порушення безпеки інформації АС не порушуючи ПРД.

Примушення будь-якого обчислювального процесу до виконання непередбаченої його розробниками роботи базується на застосування методів, способів, прийомів експлуатації потенційно-небезпечних дефектів проектування та програмної реалізації [9-10]. Існує чимало прикладів непередбаченого розробниками зовнішнього впливу на програми під час виконання, наслідками якого, як правило, є: аварійне завершення роботи, нав'язування виконання стороннього коду, розширення повноважень атакуючого, непередбачена модифікація даних і витік інформації. Найбільш репрезентативними класифікаціями відомих потенційно-небезпечних дефектів програм, умов, способу їх експлуатації, а також можливі наслідки у формі структурованих, розрахованих на фахівців шаблонів вважаються проекти CommonVulnerabilityEnumeration, CommonWeaknessEnumeration, CommonAttackPatternEnumerationandClassification [11-13].

Постановка завдання

Відомо, що головна мета політики безпеки АС полягає у розробці та впроваджені такої організації обробки інформації при якій буде мінімізована величина потенційних збитків від можливих загроз спираючись на функціонування диспетчера доступу щодо суворого

дотримання ПРД у ході експлуатації АС. При цьому існуючи положення нормативних документів технічного захисту інформації в комп'ютерних система від несанкціонованого доступу лише торкаються або розглядають поверхнево принцип коректної роботи програмного забезпечення АС, вважаючи його як самозрозуміле, нормальне припущення.

Останньому суперечить світовий досвід розслідування інцидентів інформаційної безпеки в комп'ютеризованих системах: значна кількість порушень політики безпеки інформації є результатом цілеспрямованої зловмисної діяльності непривілейованих авторизованих користувачів на деякому етапі експлуатації АС із застосуванням штатних, спеціальних програмних засобів непередбаченого розробниками впливу на алгоритм роботи службових обчислювальних процесів на основі експлуатації потенційно-небезпечних дефектів їх проектування та програмної реалізації. Примушуючи, таким чином, службовий обчислювальний процес до виконання непередбаченої розробниками роботи непривілейований авторизований користувач-порушник може за своєю ініціативою ініціювати внесення змін в його інформаційний домен, порушуючи тим самим прописану у політиці безпеки технологію обробці інформації на етапі експлуатації АС, але не вступаючи при цьому в конфлікт з диспетчером доступу. Дане явище будемо розглядати як безконфліктний несанкціонований доступ непривілейованого, авторизованого користувача-порушника і основну причину порушення політики безпеки інформації для фізично відокремлених від мережевого середовища передачі АС побудованих із застосуванням сучасних ОС загального призначення.

Таким чином можна констатувати, що політика безпека інформації не може бути повною, якщо вона базується тільки на суворій реалізації ПРД диспетчером доступу і без належної уваги до коректної роботи системного програмного забезпечення навіть у виділених АС. Завдяки наявності потенційно-небезпечних дефектів проектування та реалізації службових програм, утиліт (приблизно до 5-ти на 1000 рядків початкового тексту) завжди існує досить велика ймовірність безконфліктного несанкціонованого доступу з порушенням політики безпеки, але не ПРД, і, як наслідок, зменшення ефективності функціонування АС в цілому шляхом непередбаченого впливу на нормальну роботу її кібернетичної складової (обчислювальне середовище, процеси). Фактично ми бачимо вимогу практики щодо необхідності інтенсивного дослідження низки актуальних, взаємопов'язаних наукових задач виходячи з реалій інформаційної боротьби, світового досвіду розслідування інцидентів інформаційної безпеки, що, в свою чергу, дозволив виявити певні кризові явища теорії захисту інформації.

Перш за все необхідно розробити:

- змістовну і формальну постановку поняття ,,кібернетична безпека";
- модель оцінки значення показника кібернетичної безпеки для виділеної АС.

Основна частина

Виходячи з викладеного під *кібернетичною безпекою АС* будемо розуміти стан АС, в якому виключена (мінімізована) можливість виконання непередбаченої політикою безпеки інформації обчислювальної роботи. При побудові формального виразу показника кібернетичної безпеки будемо застосовувати декілька суттєвих припущень:

1. Функціонування будь-якої АС представляє собою послідовність переходів одного стану в іншій у випадкові моменти часу і може розглядатися як випадковий процес.

2. Семантика станів АС та умови переходів між станами визначаються виходячи з їх значущості для опису участі користувачів, як фізичних осіб, в організації прийнятої технології обробки інформації і адміністрування (проведення регламентних робіт), а також з урахуванням практичної реалізації принципів рольової політики безпеки в сучасних ОС загального призначення.

3. Сукупність сеансів роботи користувачів АС, запуск на виконання в їх межах обчислювальних процесів, а також їх властивості, розглядаються як потоки заявок на

обслуговування до виконуючого пристрою у термінах теорії масового обслуговування. Функція виконуючого пристрою реалізується ОС як операційне середовище користувача.

4. Будь-який непривілейований авторизований користувач АС в будь-який момент часу може розпочати цілеспрямовану зловмисну діяльність порушника виконуючи відповідну послідовність дій штатними програмними засобами або програмну реалізацію спеціального алгоритму розширення повноважень, що само по собі є порушенням політики безпеки АС враховуючи можливі наслідки. Успіх спроби розширення повноважень залежить від наданого для цього інтервалу часу. За результатами неуспішних спроб порушник удосконалює свої дії, програмні засоби наближаючись до бажаного результату.Успішною є остання спроба. У даній постановці тільки один непривілейований користувач АС може бути раптово почати слідувати цілям порушника.

5. Будемо вважати, що після завершення сеансу роботи непривілейованого користувача завершуються всі обчислювальні процеси запущені на виконання в його контексті, а АС переходить у стан в якому наявність або відсутність кібернетичної безпеки є невизначеною.

6. Адміністратор – привілейований користувач, який серед інших завдань при проведенні регламенту у межах свого сеансу забезпечує виконання всієї повноти заходів відновлення, за необхідністю, кібернетичної безпеки АС. Адміністратор має всі повноваження. У даній постановці адміністратор не може бути порушником.

7. Перехід між станами АС є результатом настання відповідних подій у термінах теорії ланцюгів Маркова: початок, завершення сеансу роботи користувача або адміністратора.

Виходячи з викладеного, в якості формального виразу показника кібернетичної безпеки АС пропонується:

$$\Re(t) = \sum_i P_i(t) \cdot \Re_i(t), \tag{1}$$

$$\Re_i(t) = 1 - P_{esc}^i(t), \tag{2}$$

де $P_i(t)$ - ймовірність i-го стану у ході функціонування АС, $\sum_i P_i = 1$; $\Re_i(t)$ - показник кібернетичної безпеки АС при перебуванні її у i-му стані; $P_{esc}^i(t)$ - ймовірність успішної спроби розширення повноважень непривілейованим авторизованим користувачем-порушником при перебуванні АС у i-му стані як результату виконання певної послідовності дій із застосуванням штатних засобів або програмної реалізації спеціального алгоритму (від англ. *privilegeescalation* - розширення повноважень).

Для визначення ймовірності i-го стану скористаємося відомими правилами [14]:

- якщо всі потоки подій пуасоновські, то випадковий процес в системі буде марковским;
- якщо число станів системи кінцеве і з кожного стану можна перейти в кожний інший за кінцеву кількість кроків, то граничні імовірності існують і не залежать від початкового стану системи;
- при постійній інтенсивності потоків подій в системі встановлюється певний граничний стаціонарний режим: система випадковим чином змінює свої стани, але ймовірність кожного з них не залежить від часу, ймовірність кожного стану є постійною.

Одним з центральних завдань теорії масового обслуговування зазвичай полягають у тому, щоб на підставі так би мовити „локальних” властивостей випадкових процесів дослідити їх стаціонарні характеристики на значно більшому інтервалі часу. Для відносно простих СМО і при деяких припущеннях відносно управляючої послідовності випадкових величин використовуються аналітичні методи. Аналітичний підхід базується на побудові марковских процесів, що описують стани системи. Рішення задачі у цьому випадку зводиться до формування та розв’язання системи рівнянь для стаціонарного розподілу як інваріантної міри [15].

Поняття виділеної АС є елементом набагато більш широкої авторської класифікації найбільш суттєвими характерними властивостями якої є:

- фізична відокремленість від будь-якого мережевого середовища передачі даних;
- одинарний найпростіший потік сеансів авторизованих користувачів;
- знання щодо удосконалення послідовності дій штатними засобами або програмної реалізації спеціального алгоритму розширення повноважень одержані шляхом аналізу неуспішних спроб між сеансами користувача-порушникане передаються.

Розглянемо порядок визначення ключових параметрів у ході побудови моделі оцінки значення показника кібернетичної безпеки для виділеної АС із застосуванням (1,2).

Граничні стаціонарні ймовірності $P_i(t)$ станів АС визначаються на підставі розміченого графу переходів ланцюга Маркова для випадкового процесу з дискретними станами і неперервним часом (рис. 1), де S_1 - стан, для якого визначена кібернетична безпекавиділеної АС, S_2 - стан, який відповідає сеансу роботи будь-якого непривілейованого авторизованого користувача виділеної АС, S_3 - стан, в якому кібернетична безпека невизначена, S_4 - стан, який відповідає сеансу роботи адміністратора.

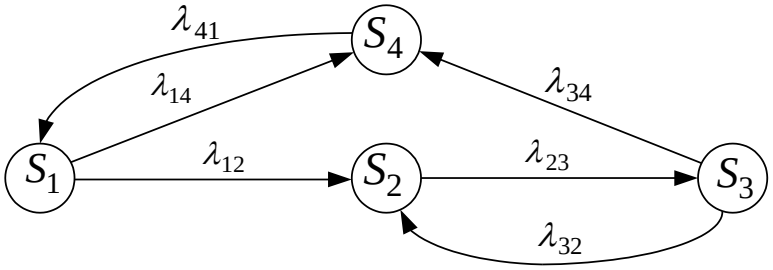

Рис. 1. Розмічений граф переходів між станами у формі ланцюга Маркова

Для складання системи рівнянь Колмогорова для виділеної АС на підставі розміченого графу переходів між станами скористуємося наступним широковідомим правилом. У лівій частині кожного рівняння записуємо похідну ймовірності стану, а у правій – кількість членів, що дорівнює кількості зв'язаних зі станом стрілок. При цьому, якщо стрілка спрямована у інший стан, то відповідний член рівняння повинен мати знак ,,мінус", якщо навпаки - ,,плюс":

$$\left.\begin{aligned}
\frac{dp_1(t)}{dt} &= -(\lambda_{14}+\lambda_{12})p_1(t)+\lambda_{41}p_4(t);\\
\frac{dp_2(t)}{dt} &= -\lambda_{23}p_2(t)+\lambda_{12}p_1(t)+\lambda_{32}p_3(t);\\
\frac{dp_3(t)}{dt} &= -(\lambda_{34}+\lambda_{32})p_3(t)+\lambda_{23}p_2(t);\\
\frac{dp_4(t)}{dt} &= -\lambda_{41}p_4(t)+\lambda_{34}p_3(t)+\lambda_{14}p_1(t).
\end{aligned}\right\} \qquad (3)$$

де $\frac{dp_1(t)}{dt}$, $\frac{dp_2(t)}{dt}$, $\frac{dp_3(t)}{dt}$, $\frac{dp_4(t)}{dt}$ - похідні ймовірностей знаходження виділеної АС у i-му стані. Визначення граничних стаціонарних ймовірностей $P_i(t)$ шляхом розв'язання системи рівнянь Колмогорова здійснюється за стандартною процедурою. Враховуючи раніше наведені припущення справедливо прийняти $P_{esc}^1(t)=P_{esc}^3(t)=P_{esc}^4(t)=0$.

Ймовірність успішної спроби розширення повноважень непривілейованим авторизованим користувачем-порушником $P_{esc}^{i}(t)$ при перебуванні виділеної АС у i-му стані шляхом виконання певної послідовності дій із застосуванням штатних засобів або програмної реалізації спеціального алгоритму визначається на підставі на основі експонентного розподілу використовуючи в якості параметру t , як правило, середню тривалість сеансу роботи непривілейованого авторизованого користувача.

Експонентний розподіл $P_{esc}^{i}(t) = 1 - \mathrm{e}^{-\lambda t}$, $t \geq 0$, $\lambda > 0$ є частковим випадком розподілу Вейбулла при $\delta = 1$[15-16] який характеризується функцією:

$$F_{\omega}(t, \delta, \sigma, \theta) = \begin{cases} 1 - \exp\left\{ -\left(\dfrac{t - \alpha}{\sigma} \right)^{\delta} \right\} & \text{при } t > 0 \\ 0 & \text{при } t \leq \theta \end{cases}.$$

де δ - параметр форми кривої розподілу, σ - параметр масштабу, α - параметр зсуву. Суттєвою властивістю розподілу Вейбулла є можливість задати монотонний спад інтенсивності спроб при $\delta < 1$ або їх монотонне зростання – при $\delta > 1$.

Висновки

Не слід забувати про те, що експонентний розподіл є ідеалізованою моделлю. Його найчастіше використовують для апріорного аналізу при порівнянні різноманітних варіантів побудови системи завдяки відносній простоті і наочності. На стадії апостеріорного аналізу повинна проводитися перевірка відповідності експонентної моделі результатам випробувань.

Література

1. Бірюков В.О., Єсаулов М.Ю., Жук П.В., Міночкін А.І., Павлов І.М. Теоретичні основи інформаційної боротьби в сучасних війнах, воєнних конфліктах та у війнах майбутнього/ – Підручник. – К.: ВІТІ ДУТ. – 2013. –322 с.

2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

3. Воєнна політика, безпека і стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення: Військовий стандарт ВСТ 001.004.004 – 2014 (1). – Київ: Міністерство оборони України, 2104. – 22 с.

4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.

5. Антонюк А.О., Жора В.В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А.О. Антонюк, В.В. Жора. – Ірпінь: національний університет ДПС України, 2010. – 310 с.

6. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій: Навч. посібник. – К.: ДУІКТ, 2009 – 450 с

7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002 –99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.

8. Таненбаум Э. Современные операционные системы. 3-е изд. – СПб.: Питер, 2012. – 1120 с.: ил. – (Серия «Классика computer science»).

9. Ховард М., Лебланк Д., Виега Д. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок . – М.: Издательский дом ДМК-пресс, 2006. – 288 с.: ил.

10. Эриксон Дж. Хакинг: искусство эксплойта. 2-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2010. – 512 с., ил.

11. CommonVulnerabilityEnumeration // – Режим доступу: http://cve.mitre.org (9.03.2015).

12. CommonWeakness Enumeration // – Режим доступу: http:// cwe.mitre.org (9.03.2015).

13. Common Attack Pattern Enumeration and Classification // – Режим доступу: http://capec.mitre.org(9.03.2015).

14. Абчук В.А. Справочник по исследованию операций / Под общ. ред. Ф.А. Матвейчука – М.: Воениздат, 1979. – 368 с. ил.

15. Математическая энциклопедия. Ред. коллегия: И.М. Виноградов (глав. ред.) [и др.] Т.1 – М., «Советская энциклопедия», 1977 т.1. А–Г. 1977. 1152 стб. с илл.

16. Левин Б.Р. Теория надежности радиотехнических систем (математические основы). Учебное пособие для вузов . М., «Сов. радио», 1978, 264 с.

Надійшла 23.02.2015 р. Рецензент: д.т.н., проф. Горбенко І.Д.