УДК 004.056 к.т.н., доц. **Стрельбіцький М.А.** (НАДПСУ)

ВИЗНАЧЕННЯ ПОКАЗНИКА УРАЗЛИВОСТІ ДАНИХ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА СТАДІЇ МОДЕРНІЗАЦІЇ

У статті наведені вихідні дані та сформульовані аналітичні залежності визначення узагальненого показника уразливості даних на стадії модернізації відомчих інформаційно-телекомунікаційних систем. На підставі наведеної моделі процесу порушення цілісності інформації на елементі інформаційно-телекомунікаційної системи визначено функціональну залежність складової узагальненого показника – цілісності. Враховуючи наведені припущення в статті досліджено питання порушення конфіденційності даних тільки у випадку сумісного використання даних різних версій програмного забезпечення. Разом з тим, складову узагальненого показника уразливості даних - спостереженість частково виражено через показники доступності, конфіденційності та цілісності.

Ключові слова: показник уразливості, захист інформації, інформаційна система

Вступ. По мірі розвитку і розширення сфери застосування обчислювальної техніки все більша частина діяльності державних органів та силових відомств приходиться на автоматизовану обробку інформації. Автоматизовані системи управління, інформаційно-телекомунікаційні системи розгорнуті, як правило, на інтранет мережах відповідних відомств та мають досить велику кількість підсистем які розподілені на всій території держави. Особливістю таких систем є вимога функціонування в реальному масштабі часу. При чому, навіть незначний збій або зупинка у функціонуванні може призвести до серйозних збитків національного масштабу. Прикладом таких систем є: інтегрована інформаційно-телекомунікаційна система прикордонного відомства "Гарт" [1], інтегрована міжвідомча автоматизована система обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон "Аркан" [2], тощо.

Життєвий цикл (ЖЦ) таких систем, як зразка озброєння і військової техніки представлений у вигляді сукупності взаємопов'язаних процесів послідовної зміни його стану протягом певного інтервалу часу з невизначеною заздалегідь тривалістю [3]. Типовий ЖЦ охоплює такі стадії: дослідження й обґрунтування розробки; розробка; виробництво; експлуатація; капітальний ремонт; списання [4]. Враховуючи, що ключовим елементом таких систем є програмні засоби, розглянемо їх ЖЦ: розробка вимог або технічного завдання; розробка системи або технічного проекту; програмування або робоче проектування; пробна експлуатація; супровід та модернізація; зняття з експлуатації [5]. Наочно, що стадії ЖЦ чітко співвідносяться один з одним.

Однією із проблем ЖЦ систем реального часу є процес модернізації системи в цілому (програмних і апаратних складових), який здійснюється поелементно до тих пір, поки не буде завершений. Як показують дослідження в галузі наукового оцінювання якості прикладного програмного забезпечення (ПЗ), біля 50% помилок виникає на стадії конструювання, які повинні бути усунуті до впровадження на робочій системі [6]. Основним способом перевірки якості створення або модернізації ПЗ є тестування, але масштаби відомчих інформаційних систем не дозволяють розгорнути їх аналог в тестовому варіанті.

В системах такого типу циркулює інформація службового характеру, що вимагає розробки та впровадження системи захисту. Разом з тим, постійне вдосконалення засобів обчислювальної техніки передбачає якісні та кількісні зміни інформаційно-телекомунікаційних систем (ІТС). Таким чином, інтеграція нових та старих засобів обчислювальної техніки та програмного забезпечення призводить до необхідності перенесення відпрацьованих роками функціональних задач, алгоритмів їх вирішення та механізмів забезпечення безпеки в нове програмно-апаратне середовище. В результаті утворюється загальне поле даних, яке використовується як старими так і новими компонентами автоматизованих систем. На цій стадії життєвого циклу системи виникає задача переходу на нову програмно-апаратну платформу без порушення життєвого циклу,

при цьому для відомчих інформаційних мереж однією із найважливіших задач є забезпечення системного захисту інформації.

Метою статті є визначення аналітичних залежностей складових узагальненого показника уразливості даних в інформаційно-телекомунікаційних системах та стадії модернізації.

Результати дослідження. Показник уразливості даних є однією зі складових інтегральної оцінки якості структури і технології функціонування системи захисту інформації. Модернізація складових інформаційних систем зумовлює зростання інтенсивності потоку дестабілізуючих факторів (ДФ), що призводить до зниження надійності даних.

Приймемо ряд припущень:

1) внутрішні функції захисту даних в окремо взятих старої і нової версіях системи захисту інформації забезпечують захист від загроз, сформульованих в технічному завданні, а також виявлених в процесі випробувань;

2) ДФ діють на інформацію незалежно один від одного;

3) процес порушення цілісності в компоненті системи не залежить від порушення цілісності інформації, що надходить в загальне поле гетерогенної системи (тобто програмно-апаратне середовище не робить збоїв і помилок, що знижують надійність даних);

Згідно визначення поняття надійності інформації [7]: цілісності, конфіденційності, доступності, спостереженості - найбільш загальний вираз показника уразливості ПУ буде виглядати наступним чином:

$$ПУ = (1 - P_{ціл})(1 - P_{конф})(1 - P_{дост})(1 - P_{спост}) \quad (1)$$

де: $P_{ціл}$ – ймовірність порушення цілісності;

$P_{конф}$ – ймовірність порушення конфіденційності;

$P_{дост}$ – ймовірність порушення доступності.

$P_{спост}$ – ймовірність порушення спостереженості.

Що стосується такого аспекту надійності інформації, як доступність, то з точки зору програмного адміністрування імовірнісна оцінка недоречна з причини того, що є детермінованою за визначенням.

Визначимо імовірнісні залежності для оцінки решти трьох ключових аспектів надійності даних.

Порушення цілісності даних. Для цілісності даних на загальному полі гетерогенної ІТС небезпеку представляють зовнішні та внутрішні загрози. До зовнішніх загроз головними можна віднести два класи ДФ: віруси і помилки людей, що беруть участь в автоматизованій обробці інформації. До внутрішніх – наявність різних версій спеціального програмного забезпечення (СПЗ).

У відповідності з викладеним та з урахуванням припущення, що програмно-апаратне середовище не робить збоїв і помилок, що знижують надійність даних, загальна модель процесу порушення цілісності інформації на елементі ІТС (АРМ, серверна частина, ЦСД) представлена на рис. 1.

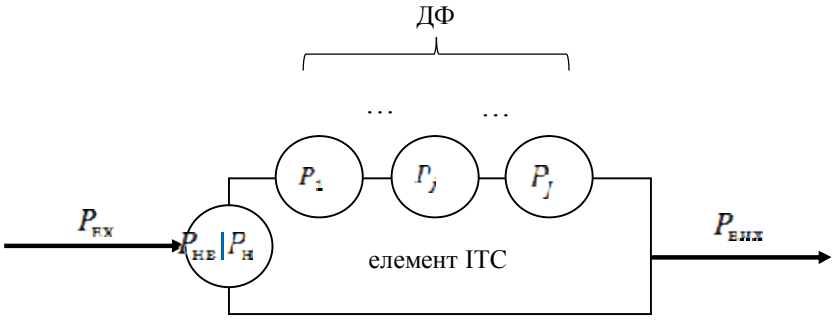

Рис. 1. Модель процесу порушення цілісності інформації на елементі ІТС

Введемо наступні позначення: ймовірність того, що дані певної категорії надходять у загальне поле елементу ІТС із старої або нової версій СПЗ з порушеною цілісністю; $P_{н}$ – ймовірність того, що дані надходять в елемент ІТС іншої версії СПЗ; – ймовірності того, що цілісність даних буде порушено в результаті неузгодженості версій СПЗ; P_j - ймовірності того що цілісність даних і-ї категорії буде порушена під впливом j-го ДФ.

Відповідно до теореми множення ймовірностей випадкових подій величина виражається наступною залежністю:

$$P_{вих} = P_{вх} + (1 - P_{вх})P_{н}P_{нв}\left(1 - \prod_{j=1}^{J}(1 - P_j)\right) \qquad (2)$$

Визначення значень $P_{н}$ можливе, як співвідношення потоку даних на вхід елементу ІТС. На рис. 2 представлено фрагмент ІТС програмно-технічного комплексу автоматизації прикордонного контролю «Гарт-1/П» із одночасним функціонуванням різних версій СПЗ (варіант).

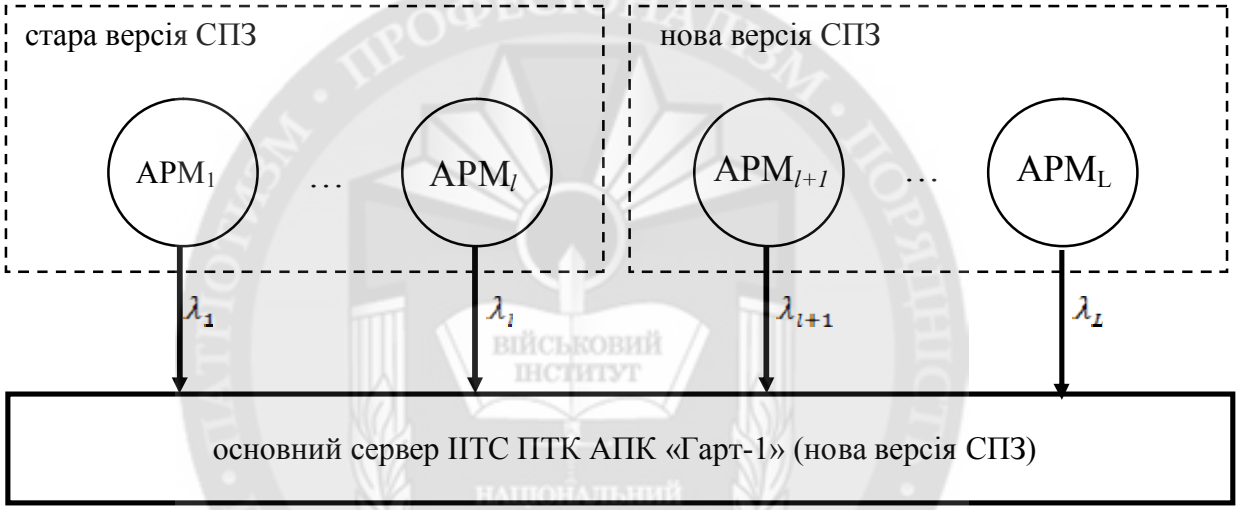

Рис. 2. Фрагмент ІТС ПТК АПК «Гарт-1» із одночасним функціонуванням різних версій СПЗ (варіант)

Таким чином, ймовірність того, що дані надходять в елемент ІТС іншої версії СПЗ є відношення потоку даних старої версії СПЗ до загального потоку даних в наступний елемент ІТС, а саме:

$$P_{н} = \frac{\sum_{i=1}^{l}\lambda_i}{\sum_{i=1}^{L}\lambda_i}. \qquad (3)$$

Визначення значень в загальному випадку є проблемним з причини неможливості врахування всієї множини вихідних параметрів старої версії СПЗ. Разом з тим, при визначенні ймовірності того, що цілісність даних буде порушено в результаті неузгодженості версій СПЗ можна застосувати метод експертних оцінок або співвідношення кількості неузгоджених параметрів до загальної кількості з урахуванням ймовірності їх застосування.

Порушення конфіденційності даних. З точки зору порушення конфіденційності даних головну небезпеку становлять злочинні дії. Зазначимо, що дослідження питання порушення

конфіденційності даних здійснюється тільки у випадку сумісного використання даних різних версій СПЗ.

Введемо наступні позначення:

$P_{\text{д}}$ – ймовірність доступу порушника до елементу ІТС;

– ймовірність наявності каналу несанкціонованого доступу (КНСД) в елементі ІТС до даних певної категорії;

– ймовірність доступу порушника до КНСД в елементі ІТС;

– ймовірність наявності даних певної категорії а елементі ІТС;

– ймовірність порушення конфіденційності при взаємодії різних версій СПЗ в елементі ІТС.

Тоді ймовірність порушення конфіденційності даних певної категорії порушником при умові надходження даних іншої версії СПЗ визначиться наступною залежністю:

$$P_{\text{к}} = P_{\text{д}} P_{\text{КНСД}} P_{\text{дк}} P_{\text{нд}} P_{\text{пк}} P_{\text{н}} . \quad (4)$$

Даний показник є базовим.

Таким чином, порушення конфіденційності даних у ІТС з урахуванням базового показника отримаємо:

$$P_{\text{к}}^{\text{ІТС}} = 1 - \prod_{i=1}^{m} \left[1 - P_{\text{к}}^{i}\right] \quad (5)$$

де – ймовірність порушення конфіденційності *k*-ї категорії даних у ІТС;

m – кількість складових, в яких може бути присутнім певна категорія даних;

$P_{\text{к}}^{i}$ – базовий показник порушення конфіденційності даних в *i*-му елементі ІТС.

Порушення спостереженості даних. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереженості [7] та визначають події, які впливають на нього, а саме: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання). Зазначимо, що розподіл обов'язків визначається керівними документами та не буде розглядатись в цій моделі.

Спостереженість даних частково можна виразити через показники доступності, конфіденційності та цілісності.

З метою визначення ймовірності порушення спостереженості даних введемо наступні позначення:

$P_{\text{р}}$ - ймовірність порушення реєстрації події щодо певної категорії даних;

$P_{\text{іа}}$ - ймовірність порушення ідентифікації і автентифікації порушника у складовій ІТС;

$P_{\text{дк}}$- ймовірність порушення достовірності каналу доступу порушником при умові доступу порушника до складової ІІТС;

$P_{\text{цкзз}}$ - ймовірність порушення цілісності комплексу засобів захисту складової ІТС.

Тоді ймовірність порушення спостереженості даних в елементі ІТС визначиться наступною залежністю:

$$P_{\text{спост}} = P_{\text{р}} P_{\text{іа}} P_{\text{дк}} P_{\text{цкзз}} \quad (6)$$

Ймовірність порушення реєстрації подій залежить від цілісності журналу обліку подій та його доступності. Зауважимо, що доступність журналу в рамках системи програмного адміністрування повинна бути постійною, тобто будь-яка подія повинна мати доступ та бути занесена до журналу, тобто .

Ймовірність порушення ідентифікації і автентифікації порушником становить:

$$P_{\text{іа}} = \left(1 - (1 - P_{\text{вих}})(1 - P_{\text{к}})\right) \prod_{m=1}^{M} P_{m}^{\text{іа}} \quad (7)$$

де $P_m^{\text{іа}}$ - ймовірність порушення ідентифікації і автентифікації m-м типом ідентифікації і автентифікації.

Ймовірність порушення цілісності комплексу засобів захисту виражається як змога протистояти множині ДФ, а саме:

$$P_{\text{цкзз}} = 1 - \prod_{j=1}^{J} \left[1 - P_j^{\text{цкзз}}\right] \quad (8)$$

Наведені вище формули цілком можуть бути використані для визначення вірогідності порушення цілісності та несанкціонованого отримання інформації. Однак для цього необхідні значення вищезазначених ймовірностей для всіх ДФ.

В даний час нам невідомі чітко визначені значення цих величин. Слід зробити ще одне зауваження. Основними елементами моделі, що розробляється, є випадкові величини. Для них необхідно знати закони розподілу, що характеризують випадкові події - прояв ДФ і числові характеристики цих розподілів, а також дані про дієвість застосування різних захисних функцій СЗІ в різних умовах. Наскільки відомо, переважна кількість зазначених даних до цього часу також не сформовано.

Проте, ґрунтуючись на евристичних даних (досвід захисту, натурні експерименти, експертне оцінювання), можна використовувати дану модель для аналізу уразливості даних в потенційно можливих умовах.

Висновок. Наведені функціональні залежності дозволять визначити ступінь уразливості даних в умовах спільного функціонуванні різних версій спеціального програмного забезпечення. Це дозволить на етапі модернізації інформаційно-телекомунікаційних систем адекватно оцінити ризики порушення надійності інформації та прийняти заходи із зниження наслідків їх реалізації.

В подальшому передбачається дослідження впливу доданих функцій програмного адміністрування на оцінку уразливості даних.

ЛІТЕРАТУРА:

1. Наказ Голови Держкомкордону від 20 серпня 2002 р. № 474 "Про прийняття на озброєння військ програмних компонентів глобальної автоматизованої інформаційної системи Прикордонних військ України (шифр "Гарт")".

2. Наказ Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 3 квітня 2008 року № 284/287/214/150/64/175/266/75.

3. Системно-концептуальна модель управління життєвим циклом зразка озброєння і військової техніки / Б. О. Демідов, О. О. Хмелевська // Системи озброєння і військ. техніка. - 2005. - № 2. - С. 47-53.

4. ДСТУ В 3576–97. Експлуатація та ремонт військової техніки. Терміни та визначення. – К.: Держстандарт України, 1998. – 60 с

5. Лавріщева К.М. Програмна інженерія. – К. – 2008. – 319 с.

6. Грицюк Ю.І., Грицюк П.Ю. Сучасні проблеми наукового оцінювання якості прикладного програмного забезпечення / Науковий вісник НЛТ України. – 2015. – Вип. 25.7

7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено Наказом департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від "28" квітня 1999 р. – № 22. Із змінами згідно наказу адміністрації Держспецзв'язку від 28.12.2012 № 806

REFERENCE:
1. Nakaz Golovy Derzhkomkordonu vid 20 serpnja 2002 r. № 474 "Pro pryjnjattja na ozbrojennja vijs'k programnyh komponentiv global'noi' avtomatyzovanoi' informacijnoi' systemy Prykordonnyh vijs'k Ukrai'ny (shyfr "Gart")".
2. Nakaz Administracii' Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny, Derzhavnoi' mytnoi' sluzhby Ukrai'ny, Derzhavnoi' podatkovoi' administracii' Ukrai'ny, Ministerstva vnutrishnih sprav Ukrai'ny, Ministerstva zakordonnyh sprav Ukrai'ny, Ministerstva praci ta social'noi' polityky Ukrai'ny, Sluzhby bezpeky Ukrai'ny, Sluzhby zovnishn'oi' rozvidky Ukrai'ny vid 3 kvitnja 2008 roku № 284/287/214/150/64/175/266/75.
3. Systemno-konceptual'na model' upravlinnja zhyttjevym cyklom zrazka ozbrojennja i vijs'kovoi' tehniky / B. O. Demidov, O. O. Hmelevs'ka // Systemy ozbrojennja i vijs'k. tehnika. - 2005. - № 2. - S. 47-53.
4. DSTU V 3576–97. Ekspluatacija ta remont vijs'kovoi' tehniky. Terminy ta vyznachennja. – K.: Derzhstandart Ukrai'ny, 1998. – 60 s
5. Lavrishheva K.M. Programna inzhenerija. – K. – 2008. – 319 s.
6. Grycjuk Ju.I., Grycjuk P.Ju. Suchasni problemy naukovogo ocinjuvannja jakosti prykladnogo programnogo zabezpechennja / Naukovyj visnyk NLT Ukrai'ny. – 2015. – Vyp. 25.7
7. Kryterii' ocinky zahyshhenosti informacii' v komp'juternyh systemah vid nesankcionovanogo dostupu ND TZI 2.5-004-99. Zatverdzheno Nakazom departamentu special'nyh telekomunikacijnyh system ta zahystu informacii' sluzhby bezpeky Ukrai'ny vid "28" kvitnja 1999 r. № 22. Iz zminamy zgidno nakazu administracii' Derzhspeczv'jazku vid 28.12.2012 № 806.

Рецензент: д.т.н., доц. Лисий М.І., науково-дослідний інститут Державної прикордонної служби України

к.т.н., доц. Стрельбицкий М.А.

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЯ УЯЗВИМОСТИ ДАННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ НА СТАДИИ МОДЕРНИЗАЦИИ

В статье приведены исходные данные и сформулированы аналитические зависимости определения обобщенного показателя уязвимости данных на стадии модернизации ведомственных информационно-телекоммуникационных систем. На основании приведенной модели процесса нарушения целостности информации на элементе информационно-телекоммуникационной системы определено функциональную зависимость составляющей обобщенного показателя - целостности. Учитывая приведенные предположения в статье исследованы вопросы нарушения конфиденциальности данных только в случае совместного использования данных различных версий программного обеспечения. Вместе с тем, составляющую обобщенного показателя уязвимости данных - наблюдаемость частично выражено через показатели доступности, конфиденциальности и целостности.

Ключевые слова: показатель уязвимости, защита информации, информационная система

Ph.D. Strelbitskiy M.A.

DEFINITION OF INDICATORS OF VULNERABILITY DATA INFORMATION AND TELECOMMUNICATION SYSTEMS ON MODERNIZATION STAGE

The article presents the initial data and analytical depending on the definition of a generalized indicator of vulnerability data at the stage of modernization of departmental information and telecommunication systems. Based on the model of the process violation the integrity of information on an item of information and telecommunication systems defined functional dependence of the generalized component index - integrity. Given the assumptions presented in the article the question of violations of privacy only when sharing data from different software versions. However, part of the generalized indicator of vulnerability data – accountability partly expressed by indicators of availability, confidentiality and integrity.

Keywords: vulnerability index, information security, information system.