ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2020.2(61)
Issue 2(61) 2020

УДК 004.056

Ткач Юлія Миколаївна,
доктор педагогічних наук, доцент,
завідувач кафедри
Національного університету
"Чернігівська політехніка",
ORCID ID 0000-0002-8565-0525

МОДЕЛІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СФЕРИ ДЕРЖАВИ

У статті проведено аналіз основних завдань захисту інформації. Побудовано моделі впливів на інформацію, оцінки вразливості інформації, що захищається, та запропонована модель нейтралізації загроз. За допомогою емпіричного підходу встановлено залежності між потенційно можливим збитком, коефіцієнтами, що характеризують частоту прояву відповідної загрози, та значенням розміру збитку, який виникає у разі її прояву. У результаті отримано вартісну модель можливих утрат. Сформульовано рекомендації щодо використання моделей.

***Ключові слова**: модель впливів на інформацію, оцінки вразливості інформації, нейтралізації загроз, інформаційна безпека держави.*

В статье проведен анализ основных задач защиты информации. Построены модели воздействий на информацию, оценки уязвимости защищаемой информации, и предложена модель нейтрализации угроз. С помощью эмпирического подхода установлены зависимости между потенциально возможным ущербом, коэффициентами, характеризующими частоту проявления соответствующей угрозы, и значением размера ущерба, возникающего при ее проявлении. В результате получена стоимостная модель возможных потерь. Сформулированы рекомендации по использованию предложенных моделей.

***Ключевые слова**: модель воздействий на информацию, оценки уязвимости информации, нейтрализации угроз, информационная безопасность государства.*

Вступ

Вирішення питань, пов'язаних із впровадженням і використанням систем моніторингу систем передачі даних (СПД), відповідно до рекомендацій Європейського Союзу (ЄС), має здійснюватися СБУ та ССЗЗІ в тісній взаємодії із провайдерами України.

Вирішення проблеми конфіденційності у приватному порядку означає, що вона має забезпечуватися за рахунок впровадження на кожному робочому місці або в корпоративній системі загалом комплексу технічних і криптографічних засобів, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею або її модифікації, відповідно до обраних стандартів конфіденційності (наприклад, PPP – Platform for Privacy Preferances).

Однак у межах держави це завдання значно ускладнюється й вимагає введення системи конфіденційного зв'язку, що одночасно вирішував би зазначені вище

проблеми, а також гарантовано надавав свої послуги корпоративному приватному сектору. Саме таким чином і вирішена ця проблема в Україні.

Метою статті є аналіз системи забезпечення безпеки в інформаційній сфері держави і розроблення моделей та методів захисту інформаційних систем.

Наукова новизна роботи полягає в розробленні моделей впливів на інформацію, оцінки вразливості інформації, що захищається, нейтралізації загроз, вартісної моделі втрат та формулюванні рекомендацій щодо їх використання.

Виклад основного матеріалу

Національна система конфіденційного зв'язку – сукупність спеціальних систем (мереж) зв'язку подвійного призначення, які за допомогою криптографічних й/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади й органів місцевого самоврядування, створюють належні умови для їхньої взаємодії в мирний час й у випадку введення надзвичайного й військового стану. Суб'єкти Національної системи конфіденційного зв'язку – органи державної влади й органи місцевого самоврядування, юридичні й фізичні особи, які беруть участь у створенні, функціонуванні, розвитку й використанні цієї системи [1, с. 127].

Основними завданнями захисту інформації є захист інформації з обмеженим доступом від витоку технічними каналами, від НСД, захист цілісності та доступності відкритої інформації, захист персональних даних. Водночас цілісність, доступність та конфіденційність інформації має забезпечуватися як під час обробки, так і під час передачі та зберігання. Вимоги до градації рівнів захисту інформації (наприклад, вимоги відсутні, низькі, середні, високі, дуже високі тощо) залежать від вимог із забезпечення безпеки кожної з властивостей інформації (конфіденційна інформація, ДСК, таємно, цілком таємно, особливої важливості). Для переведення якісних характеристик (оцінок) у кількісні величини можна використати таблицю 1 [2].

Таблиця 1

Зіставлення якісних характеристик балів-термів різноманітних шкал оцінювання знань

Бал/Терм	Якісна характеристика бала шкали оцінок				
	5-бальна	7-бальна	9-бальна	10-бальна	12-бальна
$1/T_1$	Неприйнятно	Неприйнятно	Неприйнятно	Неприйнятно	Неприйнятно
$2/T_2$	Погано	Дуже погано	Дуже погано	Дуже погано	Дуже погано
$3/T_3$	Задовільно	Погано	Погано	Погано	Погано
$4/T_4$	Добре	Задовільно (як у більшості)	Недостатньо задовільно	Недостатньо задовільно	Недостатньо задовільно
$5/T_5$	Відмінно	Добре	Задовільно	Задовільно	Задовільно
$6/T_6$	–	Дуже добре	Цілком задовільно	Цілком задовільно	Цілком задовільно
$7/T_7$	–	Відмінно	Добре	Добре	Недостатньо добре
$8/T_8$	–		Дуже добре	Дуже добре	Добре
$9/T_9$	–		Відмінно	Майже відмінно	Дуже добре
$10/T_{10}$	–			Відмінно	Недостатньо відмінно
$11/T_{11}$	–				Майже відмінно
$12/T_{12}$					Відмінно

Кількість рівнів градації шкал оцінювання може відрізнятися для кожного об'єкта. Основна вимога – забезпечення захищеності інформації на визначеному рівні.

Одним із завдань забезпечення безпеки в системі (державі) є визначення реального рівня (наприклад, високий, достатній, середній, задовільний, низький, незадовільний) зацікавленості суб'єктів, що забезпечують безпеку, у дотриманні всіх вимог до захищеності кожної з властивостей інформації.

Однак спроби несанкціонованого одержання інформації не тільки не зменшуються, а з кожним роком стають усе більш агресивними й зухвалими.

Спроба одержати НСД до інформаційної системи або обчислювальної мережі з метою ознайомлення з нею, залишити записку, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як *комп'ютерне піратство*. Як явище, подібні дії простежуються останні 20 років, але при цьому спостерігається тенденція до їхнього стрімкого зростання в міру збільшення кількості побутових персональних комп'ютерів (ПК) і створення локальних і корпоративних мереж.

Тому необхідно проаналізувати й створити модель можливого зловмисника, порушника.

Згідно із Концепцією про технічний захист інформації в Україні [3], модель порушника – опис ймовірних дій порушника, рівня його повноважень, ресурсних можливостей, програмних і (або) апаратних засобів, які він використовує з метою реалізації загроз для інформації на АТС.

Першочерговим завданням при створенні зазначених вище моделей є з'ясування об'єкта, цілей та мотивів дій зловмисника.

Залежно від мотивів, цілей і методів, дії всіх порушників можна розбити на кілька груп, починаючи з дилетантів і закінчуючи професіоналами:

– початківець;
– фахівець;
– класний фахівцем;
– фахівцем вищого класу (співробітники закордонних спецслужб).

Концепцією [3] передбачається, що порушник – суб'єкт є кваліфікованим фахівцем, володіє всією технічною інформацією про АТС і, зокрема, про системи і можливі засоби її захисту, а порушник – випадкова подія має найгірший (із позицій власників інформації, що захищається) закон розподілу.

Відносно моделі порушника будемо припускати, що порушник це фахівець вищого класу. Виходячи із цього, можна зробити висновок, що, якщо прийнята концепція правильна, то ми можемо підняти вимоги до системи захисту якнайвище.

Кожна зі сторін захисту розробляє власну модель порушника відповідно до своїх вимог.

Оскільки, порушник є фахівцем вищої кваліфікації, то він знає все про інформаційні системи, і зокрема, про склад і засоби захисту.

Отже, модель порушника визначає [4, с. 410]:

– категорії осіб, серед яких може виявитися порушник;
– можливі цілі порушника і їхню градацію за ступенем важливості й небезпеки;

– пропозиції щодо його кваліфікації;
– оцінку його технічної озброєності;
– обмеження й пропозиції щодо характеру його дій.

На підставі проведених нами досліджень наявних моделей порушника сформуємо *модель впливів на інформацію* й модель *оцінки уразливості інформації, що захищається*.

Узагальнена *модель впливів на інформацію* в автоматизованих системах обробки даних й інформаційних системах наведена на рис. 1.

Ця модель деталізується на кожному етапі та для кожного типу прояву уразливості інформації (порушення фізичної цілісності, несанкціонованого одержання, несанкціонованого розмножування або порушення логічної цілісності). При деталізації узагальненої моделі можуть бути побудовані окремі моделі для кожного з її елементів.

Практика засвідчила, що переважна більшість впливів на інформацію у випадку технічних й програмних несправностей носить випадковий характер (відмова, збій, помилка компонентів систем обробки даних, вірусне зараження тощо), можна навіть стверджувати про їх системність. Навмисна причина впливу на інформацію притаманна людині (злочинні дії) та може мати джерелом виникнення як суб'єктивні, так і об'єктивні причини.

З погляду несанкціонованого одержання інформації, принципово важливою є та обставина, що в сучасних системах обробки даних воно можливе не тільки шляхом безпосереднього доступу до баз даних, але й багатьма шляхами, що не вимагають такого доступу. При цьому основну небезпеку становлять злочинні дії людей. Вплив випадкових факторів безпосередньо не веде до несанкціонованого одержання інформації, а лише сприяє появі каналів несанкціонованого одержання інформації, яким може скористатися зловмисник.

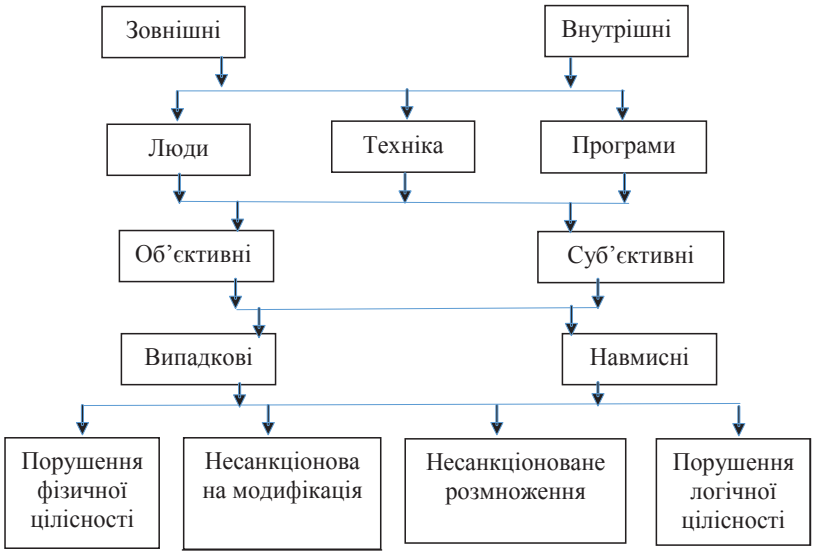

Рис. 1. Узагальнена модель впливів на інформацію

Усі зазначені компоненти моделі впливів можуть впливати на інформацію ззовні та зсередини.

Оцінимо вразливість інформації, що захищається.

У процесі розвитку теорії й практики захисту інформації сформувалися три методологічних підходи до оцінки уразливості інформації: емпіричний, теоретичний і теоретико-емпіричний. Сутність емпіричного підходу полягає в тому, що на основі тривалого збору й обробки даних про реальні прояви загроз інформації й про розміри збитку суто емпіричним шляхом установлюються залежності між потенційно можливим збитком і коефіцієнтами, що характеризують частоту прояви відповідної загрози й значення відповідного розміру збитку [1, с. 158].

Скористаємось емпіричним підходом.

Сумарна вартість втрат може бути визначена за формулою:

$$C = \sum_i C_i , \tag{1}$$

де C_i – емпірична залежність окремих втрат від *i*-ої загрози інформації й дорівнює:

$$C_i = e^{(ViЧSi-4)}, \tag{2}$$

де V_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної загрози, S_i – коефіцієнт, що характеризує значення можливого збитку при її виникненні.

Таким чином, якби вдалося зібрати достатню кількість фактичних даних про прояви загроз та їхні наслідки, то розглянуту *вартісну модель втрат* можна було б використовувати для вирішення досить широкого кола завдань ЗІ, причому неважко побачити, що модель дозволяє не тільки знаходити потрібні рішення, але й оцінювати їхню точність.

Природним продовженням моделей впливу на інформацію та моделі оцінки вразливості інформації є *моделі нейтралізації загроз*, тобто моделі захисту. Найбільш загальною моделлю захисту є модель із так званою системою з повним перекриттям.

При побудові цієї моделі як вихідне взяте природне посилання, яке полягає в тому, що в механізмі захисту має утримуватися принаймні один засіб для перекриття будь-якого потенційно можливого каналу витоку інформації.

Ось у чому полягає методика формального опису такої системи:

– складається повний перелік об'єктів систем, що підлягають захисту;

– складається повний перелік потенційно можливих загроз, тобто можливих варіантів злочинних дій;

– визначається кількісна міра відповідної загрози для відповідного об'єкта;

– формується безліч засобів ЗІ в системі;

– визначається кількісна міра можливості протидій. Якщо вона перевищує рівень загрози, то система захисту достатня.

Як правило, моделі дозволяють визначати поточні й прогнозувати майбутні значення всіх показників вразливості інформації для будь-яких компонентів системи обробки даних, будь-якої їхньої комбінації й для будь-яких умов життєдіяльності системи обробки даних.

Сформулюємо деякі зауваження щодо їх використання.

1. Практично всі моделі будуються в припущення незалежності тих випадкових подій, сукупності яких утворять складні процеси ЗІ в сучасних системах обробки даних.

2. Для забезпечення роботи моделей необхідні більші обсяги таких вихідних даних, переважна більшість яких у цей час відсутня, а формування сполучене з більшими труднощами.

Розглянемо зауваження.

Перше – припущення незалежності випадкових подій, що відбуваються в системах ЗІ. Основними подіями, імітованими в моделі визначення показників уразливості, є: прояв дестабілізуючих факторів, вплив дестабілізуючих факторів на інформацію, що захищається, і вплив засобів захисту, що використовуються, на дестабілізуючі фактори. При цьому зазвичай роблять такі припущення.

1. Потенційні можливості прояву кожного дестабілізуючого фактора не залежать від прояву інших.

2. Кожен з порушників діє незалежно від інших, тобто не враховуються можливості формування коаліції порушників.

3. Негативний вплив на інформацію кожного з дестабілізуючих факторів, що виявилися, не залежить від такого ж впливу інших факторів, що виявилися.

4. Негативний вплив дестабілізуючих факторів на інформацію в одному якому-небудь компоненті системи обробки даних може привести лише до надходження на входи пов'язаних з ним компонентів інформації з порушеною захищеністю й не впливає на такий же вплив на інформацію в самих цих компонентах.

5. Кожен із засобів захисту, що використовуються, впливає на дестабілізуючі фактори й відновлювальний вплив на інформацію, незалежно від такого ж впливу інших.

6. Сприятливий вплив засобів захисту в одному компоненті системи обробки даних лише знижує ймовірність надходження на входи пов'язаних з ним компонентів інформації з порушеною захищеністю й не впливає на рівень захищеності інформації в самих цих компонентах.

У дійсності ж події, зазначені вище, є залежними, хоча ступінь залежності різний: від незначної, якою цілком можна зневажити, до істотної, котру варто враховувати. Однак для вирішення цього завдання на сьогодні відсутня достатня кількість вхідних даних, тому ефективними залишаються лише методи експертних оцінок.

Друге зауваження стосується забезпечення моделей необхідними вихідними даними. Раніше вже неодноразово зазначалося, що для практичного використання моделей визначення показників уразливості необхідні більші обсяги різноманітних даних, причому переважна більшість із них у цей час відсутня.

Висновки

Підіб'ємо підсумки і сформулюємо рекомендації з використання моделей, розроблених у межах розглянутих раніше припущень, маючи на увазі, що це використання забезпечує вирішення завдань аналізу, синтезу й керування в системах захисту інформації і не має приводити до істотних похибок.

Перша й основна рекомендація зводиться до того, що моделями мають користуватися кваліфіковані фахівці – професіонали у сфері захисту інформації, які могли б у кожній конкретній ситуації вибрати найбільш ефективну модель і практично оцінити ступінь адекватності отримуваних рішень.

Друга рекомендація полягає в тому, що моделі потрібно використовувати не просто для одержання конкретних значень показників уразливості, а для оцінки поводження цих значень при варіюванні істотно значимими вихідними даними в можливих діапазонах їхніх змін. У цьому плані моделі визначення значень показників уразливості можуть бути досить цінним інструментом при проведенні ділових ігор із захисту інформації.

Третя рекомендація зводиться до того, що для оцінки адекватності моделей, вихідних даних й одержуваних рішень потрібно якомога ширше залучати кваліфікованих і досвідчених експертів.

Четверта рекомендація полягає в тому, що для ефективного використання моделей потрібно безупинно слідкувати за вихідними даними, необхідними для забезпечення моделей при вирішенні завдань захисту. Істотно важливою при цьому є та обставина, що гнітюча кількість вихідних даних має високий ступінь невизначеності. Тому потрібно не просто формувати необхідні дані, а перманентно оцінювати й уточнювати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Аникин И.В., Глова В.И., Нейман Л.И.* и др. Теория информационной безопасности и методология защиты информации: учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008. С. 358.

2. *Камишин В.В.* Дефазифікація бальних шкал для отримання коефіцієнтів бажаності їх оцінок. URL: file:///C:/Users/User/Downloads/Otros_2013_11_13.pdf (дата звернення: 12.05.2020).

3. Концепція про технічний захист інформації в Україні. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101957&cat_id=89734&ctime=1344502234418 (дата звернення: 13.05.2020).

4. *Остапов С.Е., Євсеєв С.П., Король О.Г.* Технології захисту інформації: навчальний посібник. Харків: Вид. ХНЕУ, 2013. 476 с.

REFERENCES

1. *Anykyn, Y.V., Hlova, V.Y., Neiman, L.Y. & Nyhmatullyna, A.N.* (2008) Teoriya informatsionnoy bezopasnosti i metodologiya zashchity informatsii. "Information Security Theory and Information Protection Methodology". Kazan. 358 p. [in Russian]

2. Kamyshyn, V.V. Defazyfikatsiya balnykh shkal dlya otrymannya koefitsiyentiv bazhanosti yikh otsinok. "Defasification of Score Scales to Obtain the Coefficients of Desirability of Their Assessments". URL: file:///C:/Users/User/Downloads/Otros_2013_11_13.pdf (Date of Application: 12.05.2020) [in Ukrainian].

3. Kontseptsiya pro tekhnichnyy zakhyst informatsiyi v Ukrayini. "The Concept of Tchnical Protection of Information in Ukraine". URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/

article?showHidden=1&art_id=101957&cat_id=89734&ctime=1344502234418 (Date of Application: 13.05.2020) [in Ukrainian].

4. *Ostapov, S.Ye., Yevseiev, S.P. & Korol, O.H.* (2013) Tekhnolohiyi zakhystu informatsiyi. Information Security Technologies: textbook. Kh.: KhNEU. 476 p. [in Ukrainian].

UDC 004.056

Tkach Iuliia,
Doct. Sci. (Pedagogy), associate professor,
Head of the Department of the National University
"Chernihivska Politekhnika"
ORCID ID 0000-0002-8565-0525

MODELS OF THE SYSTEMS OF PROTECTION OF INFORMATION SPHERE OF THE STATE

The analysis of the main tasks of information protection shows that one of the tasks of security in the system (state) is to determine the real level of interest of security entities in compliance with all requirements for security of each property of information (eg, high, sufficient, medium, satisfactory, low, unsatisfactory). Since the vast majority of influences on information in case of technical and software malfunctions (failure, failure and error of data processing system components, virus infection, etc.) are accidental, we can even say about their systemic nature, the intentional cause of information impact is human (criminal actions) and can become the main source of both subjective and objective reasons. Models of influences on information, estimations of vulnerability of the protected information are constructed, and the model of neutralization of threats (ie model of protection) is formulated. To build a model of neutralization of threats, a system with full overlap was used and a method of formal description of such a system was described. Using an empirical approach, namely on the basis of long-term collection and processing of data on the actual manifestations of information threats and the size of the damage that occurred, the relationship between potential damage and coefficients characterizing the frequent occurrence of the threat and the value its manifestation of the amount of damage, thus obtaining a cost model of losses is considered. General remarks on the use of models are formulated. First, almost all models are built with the assumption of independence of those random events, the totality of which form a complex process of information protection in modern data processing systems. Secondly, to ensure the operation of the models, larger amounts of such initial data are needed, the vast majority of which are currently absent, and the formation is associated with greater difficulties.

Keywords: model of influences on information, assessments of information vulnerability, neutralization of threats, information security of the state

Отримано 25.05.2020