Ігор Павлов
ВІТІ НТУУ "КПІ"
УДК 004.415.056.5 (075)

АНАЛІЗ УРАЗЛИВОСТЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація: **Розглядається місце і роль уразливостей в системах захисту інформації. Пропонується класифікація уразливостей систем захисту інформації та розкривається її зміст.**
Summary: **We consider the position and role of vulnerabilities in information security systems, a classification of vulnerabilities of information security systems and disclosed its contents.**
Ключові слова: **Аналіз, загрози, механізми захисту, модель, система захисту інформації, уразливості.**

I Вступ

Аналіз існуючих публікацій, пов'язаних з проблемою проектування систем захисту інформації, показує недостатнє освітлення системних підходів до проблеми опису уразливостей систем захисту інформації [1–7].

Проводячи різні оцінки ефективності моделей захисту інформації дослідники спираються на відірвані підходи до аналізу уразливостей тих або інших систем захисту.

У зв'язку з цим виникає об'єктивна необхідність визначення основних підходів у вивченні процесів, які виникають в областях уразливостей систем захисту інформації під час впливу небезпечних для цих систем загроз. Для цього необхідно визначити місце і роль уразливостей у математичній моделі, провести класифікацію уразливостей для подальшого використання системного підходу аналізу уразливостей систем захисту інформації в оцінках ефективності моделей, які будуються на етапі проектування систем захисту інформації. Загальною основою для проведення цього аналізу є модель процесу захисту інформації з повним перекриттям загроз.

II Основна частина

Місце і роль уразливостей у математичній моделі процесу захисту інформації з повним перекриттям загроз

Для визначення місця та ролі областей уразливості систем захисту інформації розглянемо типову модель процесу захисту інформації з повним перекриттям загроз, зображену на рис. 1 [7, 8].

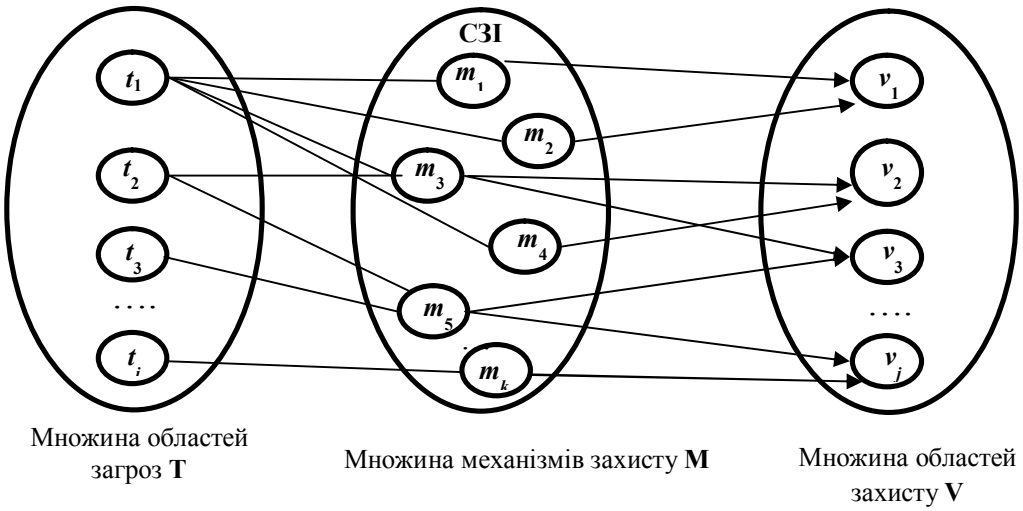

Рисунок 1 – Типова модель процесу захисту інформації з повним перекриттям загроз

В цій моделі існує три основних множини:

T = {ti} – множина загроз інформації, де i – кількість загроз, $i = \overline{1, I}$;

V = {vj} – множина об'єктів (ресурсів), які захищаються, де j – кількість ресурсів, які захищаються, $j = \overline{1, G}$;

M = {mk} – множина механізмів захисту, де k – кількість механізмів захисту, $k = \overline{1, K}$.

Елементи цих множин знаходяться у визначених взаємовідношеннях.

В механізмах захисту – mk, системи захисту інформаці M, існують наступні області.

1. Області уразливості механізмів захисту U, на які впливають загрози системи захисту інформації.

2. Бар'єри захисту B, які встановлюються в системі захисту для блокування загроз, що впливають на області ураження системи захисту.

Отже, система захисту інформації розглядається як сукупність місць уразливості системи та бар'єрів, що блокують ці небезпечні області:

$$\mathbf{M} = \{m_k\} = \{\mathbf{U} \times \mathbf{B}\}. \tag{1}$$

Необхідно враховувати ще дві сукупності, що входять у множину механізмів безпеки (системи захисту) [8]:

U = {ur} – набір уразливих місць системи захисту, де r – кількість уразливих місць, $r = \overline{1, R}$;

B = {bg} – набір бар'єрів захисту, які є в системі захисту, g – кількість бар'єрів захисту, $g = \overline{1, G}$;

Із урахуванням цього, модель захисту інформації в автоматизованій мережі з повним перекриттям має вигляд, приведений на рис. 2.

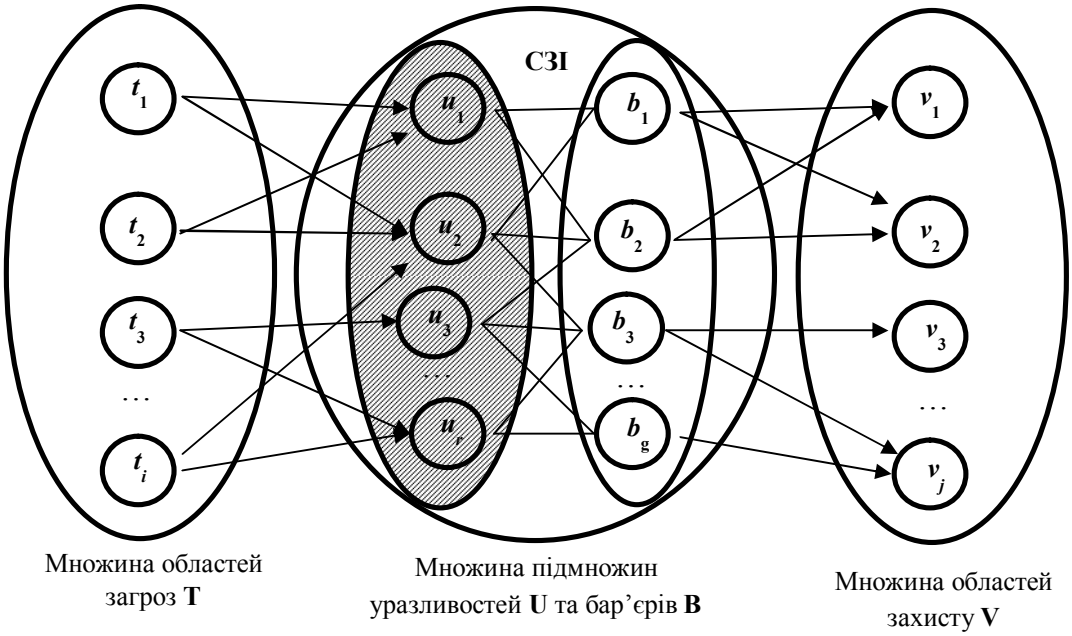

Рисунок 2 – Місце і роль уразливостей у типовій моделі процесу захисту інформації з повним перекриттям загроз

Елементи підмножин U і B знаходяться у визначених взаємовідношеннях: кожній уразливості відповідає набір бар'єрів [b1, …, bp], де p – кількість бар'єрів, $p = \overline{1, P}$.

Можна записати, що для системи з повним перекриттям виконується умова:

$$\forall < \text{ti, vj} > \in \text{M} \; \exists \; \{<\text{ur, bg}> \mid f\ (\text{ti, vj})\}, \tag{2}$$

де функціонал f (ti, vj) – описує виконання умови забезпечення захисту об'єкта vj за наявності загрози ti .

Таким чином, для системи захисту з повним перекриттям для всіх загроз існують бар'єри, які перешкоджають здійсненню цих загроз.

Вплив загроз аналітично можна описати у вигляді функціональних залежностей, які зв'язують характеристики загроз ti∈T та об'єкти захисту vj ∈V.

Кожна з величин vj∈V залежить від r – координат уразливостей та g – координат бар'єрів. Ступінь залежності величин vj залежить від уразливостей ur∈U та бар'єрів bg∈B і визначається відповідно до передатних функцій $a_{ik}(p),\ c_{ik}(p),\ d_{ik}(p),$ де p – оператор Лапласа, як наведено в (3).

Система рівнянь (3) повністю характеризує систему захисту інформації. Вона показує вплив вхідних значень на області уразливості СЗІ у вигляді загроз та вихідні дані, які є внутрішніми зв'язками системи захисту інформації між областями уразливості і множиною механізмів захисту.

$$
\begin{aligned}
v_1 &= t_1\ a_{11} + t_2\ a_{12} + \ldots + t_i\ a_{1j} + \\
&+ u_1\ c_{11} + u_2\ c_{12} + \ldots + u_r\ c_{1j} + \\
&+ b_1\ d_{11} + b_2\ d_{12} + \ldots + b_g\ d_{1j}\ , \\
v_2 &= t_1\ a_{21} + t_2\ a_{22} + \ldots + t_i\ a_{2j} + \\
&+ u_1\ c_{21} + u_2\ c_{22} + \ldots + u_r\ c_{2j} + \\
&+ b_1\ d_{21} + b_2\ d_{22} + \ldots + b_g\ d_{2j}\ , \\
&\ldots\ldots\ \ldots\ldots\ \ldots\ldots\ \ldots\ldots\ \ldots\ldots\ \ldots\ \ldots\ldots\ \ldots\ldots \\
v_j &= t_1\ a_{j1} + t_2\ a_{j2} + \ldots + t_i\ a_{jj} + \\
&+ u_1\ c_{j1} + u_2\ c_{j2} + \ldots + u_r\ c_{jj} + \\
&+ b_1\ d_{j1} + b_2\ d_{j2} + \ldots + b_g\ d_{jj}\ .
\end{aligned}
\qquad (3)
$$

Усе сказане вище ставить задачу – проаналізувати уразливості систем захисту інформації для подальшої оцінки ефективності систем захисту інформації, особливо на етапі проектування, як систем захисту так і будь-яких інформаційних систем у цілому.

Класифікація уразливостей системи захисту інформації

Уразливості системи захисту інформації – це будь-які характеристики системи захисту, використання яких може привести до реалізації загроз в областях захисту моделі системи захисту інформації.

Одне з перших досліджень у цій області проводилося у рамках проекту Protection Analysis Project у середині 70-х років минулого століття [1]. Досліджувалися уразливості операційних систем. Протягом декількох років учасники проекту опубліковували декілька статей, у яких описувалися категорії уразливостей і способи їх пошуків по шаблонам. Однак запропоновані методи не могли бути легко автоматизовані, і база даних уразливостей, яка була розроблена, так і не була опублікована.

У 1996 році лабораторія COAST університету Пардью розробила свою класифікацію [2], а кампанія ISS − свою [3]. Згідно з останньою виділяють уразливості:

реалізовані або створені розробником (продавцем) програмного або апаратного забезпечення;

добавлені адміністратором у процесі управління компонентами системи;

привнесені користувачами у процесі експлуатації системи.

Деякі дослідники класифікують уразливості за етапами життєвого циклу систем захисту інформації [6], які представлені в табл. 1.

Таблиця 1 – Класифікація уразливостей по етапам життєвого циклу систем захисту інформації

Етапи життєвого циклу	Категорії уразливостей механізмів захисту
Проектування СЗІ	Уразливості проектування СЗІ
Реалізація СЗІ	Уразливості реалізації СЗІ
Експлуатація СЗІ	Уразливості конфігурації СЗІ

У [9] прослідковується проведення аналізу уразливостей за величиною збитків, які можуть бути нанесені для областей захисту інформаційної системи, або для областей захисту самої системи захисту інформації.

Але в цілому прослідковується кінцевий результат проникнення самих загроз. Така класифікація представлена в табл. 2.

Таблиця 2 – Можливості по виявленню і усуненню уразливостей СЗІ

Категорії уразливості	**Виявлення**	**Усунення**
Уразливості реалізації	Відносно важко, довго	Легко, але відносно довго
Уразливості конфігурації	Легко і швидко	Легко і швидко
Уразливості проектування	Важко і довго	Важко і довго (іноді неможливо)

Для проведення аналізу систем захисту інформації і оцінки збитків у випадку реалізації загроз збитки враховуються, як у вартісному обчисленні, так і "нематеріальні" збитки, які нанесені репутації, конкурентним можливостям.

У останньому випадку вводяться семантичні показники – "одиниці нанесення збитків" і "вірогідність нанесення збитків"; остання пов'язана з частотою реалізації загрози за визначений період часу.

Загальна класифікація уразливостей механізмів захисту інформаційних систем і в першу чергу самих систем захисту інформації представлена на рис. 3.

Рисунок 3 – Загальна класифікація уразливостей механізмів захисту систем захисту інформації

На етапах життєвого циклу уразливості проектування СЗІ, або в цілому інформаційних систем, найбільш небезпечні. Вони виявляються та усуваються з великими проблемами. У цьому випадку уразливість притаманна проекту або алгоритму, і відповідно, якщо існує ідеальна реалізація (що неможливо), то це не виключає проект або алгоритм (програму) від закладених слабких сторін і небезпечних збитків. Наприклад, уразливість стеку протоколів TCP/IP. І усунути ці проблеми вже неможливо – існують тільки тимчасові або неповні заходи. Однак є винятки. Наприклад, внесення в проект корпоративної мережі множини модемів, які полегшують роботу персоналу, але істотно ускладнюють роботу служби безпеки. Це приводить до появи потенційних шляхів обходів міжмережевих екранів, які забезпечують захист внутрішніх ресурсів від несанкціонованих використань. Але виявити та усунути такі уразливості достатньо легко.

Уразливості реалізації СЗІ проявляються у появі помилок на етапі реалізації в програмно-апаратному забезпеченні, коректному з точки зору безпеки проекту або алгоритму. Яскравим прикладом такої

уразливості є “переповнення буферу” (“buffer overflow”) у багатьох реалізаціях програм, наприклад, sendmail або Internet Explorer [1]. Усуваються подібного роду уразливості відносно легко. Якщо нема вихідного коду програмного забезпечення (ПЗ), у якому виявлена уразливість, то його усунення здійснюється або відновленням версії уразливого ПЗ або повною його заміною, або у відмовою від нього.

Уразливості конфігурації СЗІ – це помилки конфігурації програмного або апаратного забезпечення. Цей вид, поряд з уразливостями реалізації, є найрозповсюдженішим з категорій уразливостей [1]. Існує множина прикладів таких уразливостей. До їх числа можна віднести доступні, але які не використовуються на вузлі сервісу Telnet серед множини “слабких” паролів або паролів, довжиною менш 6 символів, облікові записи (accounts) і паролі, встановлені за умовчанням (наприклад, SYSADM або DBSNMP в СУБД Oracle) і т. п. Локалізувати або виправити такі уразливості можливо.

У цілому можливості з виявлення та усунення уразливостей проектування, реалізації та конфігурації СЗІ представлені в табл. 2.

Основна проблема – визначити, може бути конфігурація уразливою чи ні. За статистикою, яка проводиться інститутом SANS, кампанією ISS [3−5], існують наступні групи найбільш поширених уразливостей, представлених на рис. 4.

Рисунок 4 – Групи найбільш поширених уразливостей ПЗ інформаційних систем

Найбільш структуровано можна представити уразливості процесів проектування, реалізації та конфігурації за допомогою V – подібної моделі життєвого циклу програмного забезпечення інформаційних систем.

V − подібна модель була запропонована для того, щоб усунути недоліки ітераційної та водоспадної моделей [10]. А назву ця модель отримала за своє специфічне графічне представлення (рис. 5). В літературі ця модель ще має назву шарнірної.

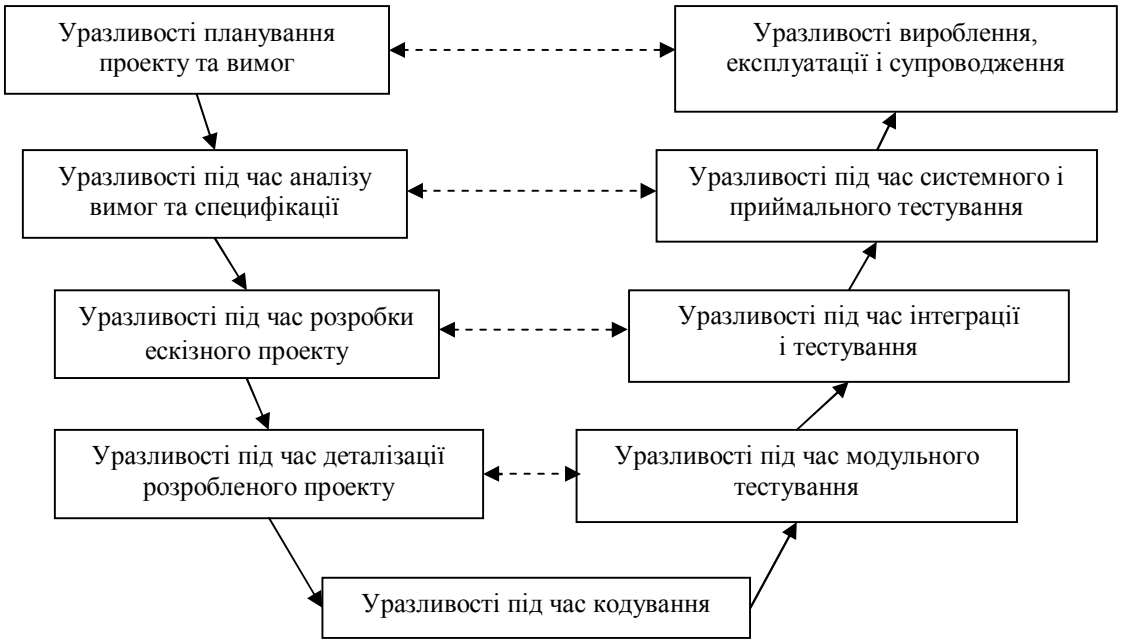

Рисунок 5 – V – подібна модель врахування уразливостей під час життєвого циклу програмних продуктів СЗІ

V − подібна модель дала можливість значно підвищити якість розробки програмних продуктів шляхом орієнтації на тестування, а також в цілому вирішила проблему відповідності створеного продукту вимогам, які надаються замовником, бо в цій моделі є процедури верифікації і атестації на ранніх стадіях розробки (пунктирні лінії рис. 5. вказують на залежність етапів планування, постановки задачі та приймання продукту).

Однак в цілому V − образна модель є модифікацією ітераційної моделі і має її недоліки. Тобто, вона також слабко пристосована до можливих змін вимог замовника. Коли процес розробки займає великий час (до років), то отриманий в результаті продукт може виявитися фактично непотрібним замовнику, оскільки його потреби істотно змінилися. Водночас актуальним є питання науково-технічного прогресу: вимоги до програмного забезпечення виходять з досягнень в області апаратно-програмного забезпечення, однак ІТ-сфера розвивається швидко, і процес розробки, який затримується, спроможний привести до створення продукту, який базується на застарілих технологіях і стає неконкурентоспроможним ще до своєї появи.

Важливим є питання планування показників функціональності, оскільки в цих моделях воно є не більше як припущення: тобто, визначити, яку швидкість обробки даних забезпечить програмний продукт, скільки він буде займати пам'яті. Коли подібні вимоги чітко фіксуються в умовах договорів між замовником і виконавцем, то таке рішення не буде задовольнятися, бо це стане відомим на завершальних етапах розробки.

За характером дій, які приводять до уразливостей інформаційних систем, розрізняють:

уразливості, які реалізовуються або створюються розробником (продавцем) програмного або апаратного забезпечення; включають: помилки, які не встановлені під час оновлення операційних систем, уразливі сервіси, незахищені конфігурації;

уразливості, які добавлені адміністратором у процесі управління компонентами системи; включають: доступні налагодження, параметри системи, які або неправильно використовуються, або не відповідають політиці безпеки;

уразливості, які привнесені користувачами в процесі експлуатації системи; включають: відмови або відхід від прийнятої політики безпеки.

За характером збитків для інформаційних систем уразливості можна прив'язати до величини нематеріальних збитків, та частоти реалізації загрози. Семантичні показники уразливостей за величиною збитку для систем захисту інформації представлені в табл. 3.

Таблиця 3 – Семантичні показники уразливостей за величиною збитків для систем захисту інформації

Уразливості за величиною збитку	**Семантична характеристика показника "величина нематеріального збитку"**
Суттєво малі	Збиток можна не брати до уваги
Незначні	Збиток легко відновлюється, затрати на ліквідацію реалізованої загрози невеликі
Середні	Ліквідація реалізованої загрози не пов'язана з великими втратами і не пов'язана з критично важливими задачами, але місце серед клієнтів погіршується, частина важливої інформації втрачається.
Важливі	Ускладнюється виконання критично важливих задач. Втрата на великий період важливого положення серед клієнтів. Ліквідація реалізованої загрози пов'язана зі значними фінансовими інвестиціями.
Критичні	Реалізація загрози приводить до неможливості рішення критично важливих задач. Організація перестає функціонувати.

За загальні критерії "вартість/ефективність" можна прийняти наступні вимоги:

вартість СЗІ не повинна перевищувати визначену суму (як правило, не більш 20% від вартості інформаційних технологій, які необхідно захищати);

рівень збитків не повинен перевищувати деяке значення, наприклад, незначний, як вказано у табл. 3.

Семантичні показники уразливостей за частотою реалізації загроз представлені в табл. 4 .

Таблиця 4– Семантичні показники уразливостей за частотою реалізації загроз в системах захисту інформації

Частота реалізації загроз	**Значення вірогідності**	**Семантична характеристика реалізації загрози**
Нульова	Близько нуля	Загрози практично ніколи не реалізуються
1 раз на декілька років	Доволі низька	Загрози реалізуються рідко
1 раз на рік	Низька	Скоріше всього, загрози не реалізуються
1 раз на місяць	Середня	Скоріше всього, загрози реалізуються
1 раз на тиждень	Вище середньої	Загрози обов'язково реалізуються
1 раз на день і частіше	Висока та дуже висока	Шансів на позитивній результат немає

У цілому пропонується безліч методик для вирішення необхідного оптимуму за критерієм "вартість/ефективність". Усі методики розраховані безпосередньо для кожного конкретного випадку функціонування конкретних кампаній, фірм. Частіше беруться до уваги методики експертних оцінок, які також мають масу недоліків, бо залежні від конкретних осіб, які повинні мати бездоганний досвід і масу інформації, яка не завжди може бути їм надана. Тобто, найдосвідченіші фахівці можуть приблизно представити ці данні.

III Висновки

У інформаційних системах існують різні засоби, які використовують будь-які способи блокування уразливостей систем, попередження впливу загроз на механізми захисту систем захисту інформації. Одним із перспективних напрямків є створення окремих систем виявлення загроз (системи виявлення атак, системи виявлення мережевих втручань і т. п.).

На сьогоднішній день системи виявлення вторгнень являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в комп'ютерних системах або мережах, а також самостійно аналізують ці події у пошуках ознак проблем безпеки, в тому числі проводять пошук областей уразливостей систем захисту. Такі системи реалізуються практично в усіх антивірусних системах, що проводять моніторинг програмних інформаційних технологій, встановлених в комп'ютерні системи. Але подальший напрямок розвитку систем, які будуть проводити моніторинг, виявляти та блокувати уразливості систем захисту інформації та у цілому в інформаційних системах, буде розвиватися у напрямку впровадження систем з елементами штучного інтелекту.

Список використаної літератури: ***1.*** *Лукацький А. В. Обнаружение атак. / А. В. Лукацький. – СПБ.: БХВ-Петербург. – 2001. – 632 с.* ***2.*** *Taimur Aslam.Use of A Taxonomy of Security Faults / A. Taimur, I. Krsul, H. Eugene. – 1996. – CJAST Laboratory.* ***3.*** *Анализ защищенности: сетевой или системный анализ? Руководство по выбору технологии анализа защищенности Internet Security Systems / Перевод с англ. Лукацького А. В., Цаплева Ю. Ю. – 1999.* ***4.*** *How To Tliminate The Ten Most Critical Internet Secrurity Threats. Version 1.32. SANS January 18. 2001.* ***5.*** *Chris Klaus. Top Threats Facing Internet Security Today. ISS Connect 2000. 19-24. March. 2000.* ***6.*** *Шорошев В. Перспективный метод защиты информационных ресурсов корпоративных сетей интернет / Шорошев В. – Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2003. – вип. 7. − С. 62 – 76.* ***7.*** *Лівінцев С. П. Математична модель захисту інформації в автоматизованих мережах спеціального призначення / С. П. Лівінцев, І. М. Павлов, О. І. Романов. – Збірник наукових праць ВІТІ НТУУ "КПІ". – К.: 2004. – № 5. – С. 23 – 31.* ***8.*** *Павлов І. М. Модель процесу роботи комплексної системи захисту інформації в спеціальних інформаційно-телекомунікаційних системах та вимоги до неї по захищеності інформації / І. М. Павлов. – Збірник наукових праць ВІТІ НТУУ "КПІ". – Київ: 2006. – № 3. – С. 82 – 91.* ***9.*** *Нестерук Г. Ф. К оценке защищнности систем информационных технологий / Г. Ф Нестерук, Л. Г. Осовецкий, Ф. Г. Нестерук. – Спб: 2004. − ГИТМО. С. 31 – 41.* ***10.*** *Павлов І. М. Моделі життєвого циклу програмних механізмів захисту комплексної системи захисту інформації / І. М. Павлов. − Сучасний захист інформації. – К.: 2011. − № 2. − С.60 − 68.*