COMPUTER SYSTEMS AND NETWORKS

Vol. 4, No. 1, 2022

DOI: https://doi.org/10.23939/csn2022.01.021

УДК 004.056

ПРО ОДИН ПІДХІД ДО ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ ВІД ЗОВНІШНЬОГО ВТРУЧАННЯ

В. А. Голембо

Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин,
e-mail: Vadym.A.Holembo@lpnu.ua

Розглянуто підхід до підвищення захищеності комп'ютерних систем від зовнішнього втручання. Обґрунтовано актуальність проблеми захисту інформації та кібербезпеки. Розглянуто стратегії нападу та деструктивних дій, які застосовують порушники (хакери). Виділено 16 різних стратегій нападу та порушень.

Проаналізовано причини вразливості комп'ютерних систем. Розглянуто дві групи причин: об'єктивні причини, які залежать від апаратно-програмних компонентів комп'ютерної системи, та суб'єктивні причини, які залежать від людського фактору. Зазначено, що одною з основних причин, яка об'єктивно ускладнює захист комп'ютера від зовнішнього втручання, полягає в тому, що на один і той самий комп'ютер покладають розв'язання двох непов'язаних між собою проблем: безпосереднє розв'язання задачі, що, по суті, є внутрішньою проблемою, та здійснення зв'язку, що можна розглядати як зовнішню проблему.

Запропоновано підхід до підвищення захищеності комп'ютерних систем від зовнішнього втручання шляхом апаратної надлишковості, зокрема, замість одного комп'ютера застосовувати комп'ютерний блок, який складається з двох комп'ютерів – внутрішнього і зовнішнього. Внутрішній комп'ютер використовується для розв'язання задачі. На зовнішній комп'ютер покладається виконання функцій зв'язку. Додатково розглянуто питання фізичного захисту комп'ютерних систем.

Ключові слова: захист інформації, кібербезпека, зовнішнє втручання.

Вступ

Проблема захисту комп'ютерних систем (КС) від зовнішнього втручання є надзвичайно актуальною. Хакери демонструють реальні деструктивні дії, і це не є лише вигадками журналістів. Іноді хакери просто втручаються у роботу КС, а іноді вимагають гроші за припинення втручання, і ці гроші постраждалі фірми в деяких випадках змушені платити. Своїми діями окремі хакери та хакерські групи спроможні порушувати роботу одночасно сотень компаній як у окремих країнах, так і в усьому світі. Порушення роботи компаній тягне за собою великі збитки і додаткові витрати на подолання наслідків хакерських атак [1]. Одними з найбільш небезпечних є хакерські атаки на фінансові установи та системи оплати, в тому числі мережі банкоматів та касових апаратів. Останнім часом подібні атаки стають все більш складними та масштабними [2–4]. При цьому технології захисту інформації та системи кібербезпеки в багатьох випадках програють нападникам [5–8].

Хакерські атаки приносять своїм організаторам і виконавцям великі гроші. За повідомленнями новин, у 2020 році хакери з використанням вірусів-вимагачів заробили 18 млрд доларів. Велику загрозу несуть хакерські атаки на державні установи, об'єкти інфраструктури та системи енергетики. За повідомленням агенцій новин, подібні атаки носять регулярний характер. Відтак проблема підвищення захищеності комп'ютерних систем від зовнішнього втручання заслуговує на особливу увагу.

1. Проблема захисту комп'ютерних систем

Розглянемо методи, за допомогою яких хакери організують втручання у роботу КС. Зазначимо, що існує певна аналогія між цими методами і методами криптоаналізу, які застосовуються в криптографії [9]. Одним із важливих моментів при цьому є питання термінології. Зовнішнє вторгнення в КС здійснюється порушниками, серед яких іноді виділяють хакерів і крекерів.

Хакером (hacker) називають порушника, який вторгається (проникає) в КС, як правило, з якоюсь інтелектуальною метою, наприклад, щоб показати свою спроможність зламати систему захисту. При цьому в більшості випадків він не має наміру заподіяти шкоду власнику КС. Крекером (cracker) називають порушника, який вторгається (проникає) в КС, в першу чергу, з метою заподіяти шкоду власнику КС. В останні роки всіх порушників зазвичай називають хакерами, а сам факт порушення вважають деструктивною шкідливою дією [10].

Для того, щоб ясніше розуміти необхідність надійного захисту від зовнішнього вторгнення, розглянемо різні стратегії нападу та деструктивних дій, які можуть застосовувати порушники (хакери).

1. Одержувати несанкціонований доступ, тобто порушувати таємницю або конфіденційність інформації.

2. Видавати себе за іншого користувача, щоб зняти з себе відповідальність, або використати його повноваження з метою формування неправдивої інформації, зміни законної інформації, застосування недійсного посвідчення особистості для одержання недозволеного доступу, або санкціонування неправдивих обмінів інформацією чи їх підтвердження.

3. Відмовлятись від факту формування інформації.

4. Свідчити, що інформація одержана від певного користувача, хоч насправді вона сформована самим порушником.

5. Стверджувати про те, що отримувачу (у визначений час) була надіслана інформація, яка насправді не відсилалась (або пересилалась у інший час).

6. Відмовлятися від факту отримання інформації, яка фактично була одержана, або надавати неправдиві відомості під час її отримання.

7. Несанкціоновано розширювати свої законні повноваження (на доступ, формування та розповсюдження інформації).

8. Несанкціоновано змінювати без дозволу повноваження інших користувачів (вносити до списків на обмежене користування інших осіб або розширення існуючих повноважень тощо).

9. Приховувати факти наявності деякої інформації (приховане передавання) в іншій інформації (відкрите передавання).

10. Підключатися до лінії зв'язку між іншими користувачами активним (прихованим) ретранслятором.

11. Вивчати дані про те, хто, коли і до якої інформації (джерел, фактів) має доступ (хоч сама інформація лишається закритою).

12. Висловлювати сумнів щодо протоколу забезпечення цілісності інформації шляхом її розкриття, яка згідно з умовами протоколу повинна залишатися таємною.

13. Модифікувати програмне забезпечення шляхом непомітного внесення нових функцій.

14. Примушувати інших порушувати протокол шляхом введення неправдивої інформації.

15. Підривати довіру до протоколу шляхом виклику очевидних порушень.

16. Намагатися перешкоджати передаванню повідомлень між іншими користувачами, зокрема внесенням до повідомлень прихованих завад з тією метою, щоб це повідомлення при аутентифікації не було прийнято.

2. Причини вразливості комп'ютерних систем

Проаналізуємо основні причини, які можуть негативно впливати на захищеність КС від зовнішнього втручання, яке здійснюється порушником (хакером), що територіально та юридично знаходиться за межами КС і не є її власником або співвласником.

Будемо виділяти дві групи причин: *об'єктивні* причини, які залежать від апаратно-програмних компонентів КС, та *суб'єктивні* причини, які залежать від людського фактору.

Розглянемо причини *першої* групи. Комп'ютер, який входить до складу КС і який є основним робочим інструментом користувача, виконує наступні основні функції:

– функції, які направлені на розв'язання задачі (індивідуально або в складі групи комп'ютерів, що утворюють КС),

– функції, які орієнтовані на здійснення зв'язку з керівництвом і замовниками та з іншими комп'ютерами КС, а також з комп'ютерами колег по роботі.

Очевидно, що одна з основних причин, яка об'єктивно ускладнює захист комп'ютера від зовнішнього втручання, полягає в тому, що на один і той самий комп'ютер покладають розв'язання двох непов'язаних між собою проблем: безпосереднє розв'язання задачі, що, по суті, є *внутрішньою* проблемою, та здійснення зв'язку, що можна розглядати як *зовнішню* проблему (рис. 1).

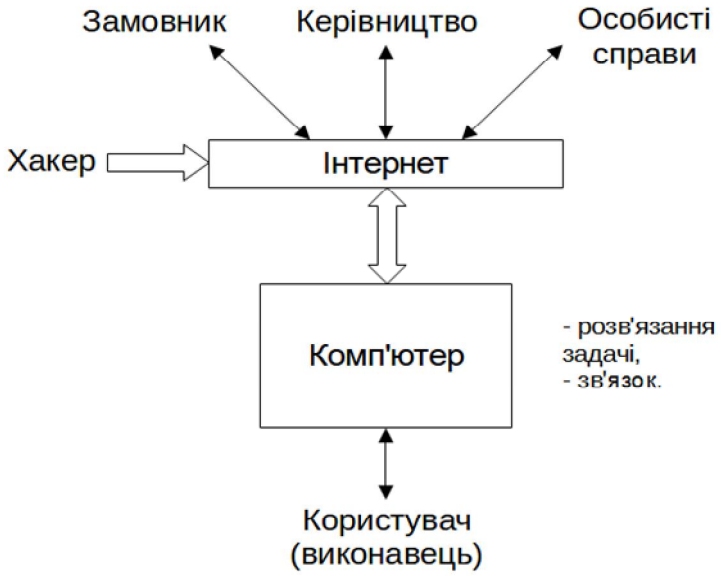

Рис. 1. Схема використання комп'ютера у складі КС

Розглянемо причин *другої* групи, які залежать від людського фактору. При роботі на комп'ютері (в складі КС) користувач використовує певні протоколи, строге (пунктуальне) виконання яких практично унеможливлює спроби хакера неконтрольовано увійти в КС або порушити її цілісність.

Але іноді спрацьовує людський фактор. Користувач, який упродовж довгого часу пунктуально виконував необхідні для захисту протоколи, бачить, що ніхто не заважає нормальній роботі КС, не робить спроб несанкціоновано увійти в КС або порушити її роботу. А строге (пунктуальне) виконання протоколів вимагає уважності і займає додатковий час. Тому користувач починає потроху спрощувати виконання протоколів, а в окремих випадках уникає їх застосування. Не виключені також випадки, коли користувач використовує комп'ютер для виконання своїх власних справ, наприклад, здійснює зв'язок з родиною та друзями, а іноді й просто розважається (дивиться фільми, грає у комп'ютерні ігри). Очевидно, що частина користувачів (співробітників) психологічно не в змозі відмовитися від використання робочого комп'ютера не за прямим призначенням.

У цій ситуації у хакера з'являються можливості для атаки. Іноді він намагається здійснити швидку атаку і, якщо відразу зламати захист не вдається, то відмовляється від подальших спроб, після чого шукає більш вдалий об'єкт для демонстрації своєї майстерності (так частіше чинить

хакер, але не крекер). Але якщо хакер виконує замовлення ворожої або конкуруючої структури, то його дії більш небезпечні, особливо в разі, якщо він більш досвідчений ніж користувач. Хакер починає "полювання" за робочим комп'ютером користувача, очікує помилки останнього, і це "полювання" відбувається, як правило, упродовж довгого часу в умовах, коли користувач не відчуває, що за його діями слідкують. Загалом дії досвідченого хакера подібні до дій снайпера, який чекає на фатальну помилку жертви.

3. Захист комп'ютерної системи шляхом апаратної надлишковості

Проведений вище аналіз об'єктивних та суб'єктивних причин, які можуть негативно впливати на захищеність КС від зовнішнього вторгнення, показав, що для кардинального розв'язання проблеми необхідний радикальний крок, який полягає у інформаційному відокремленні робочого комп'ютера від потенційного порушника (хакера), що можна досягнути шляхом введення апаратної надлишковості. Нагадаємо, що введення надлишковості для підвищення надійності будь-якої інформаційної структури було запропоновано ще в класичних роботах [11, 12].

Саме тому для забезпечення надійного захисту від деструктивних дій хакерів пропонується замість одного комп'ютера застосовувати комп'ютерний блок, який складається з двох комп'ютерів – внутрішнього і зовнішнього, розділивши між ними основні функції так: внутрішній комп'ютер використовується для розв'язання задачі, на зовнішній комп'ютер покладається виконання функцій зв'язку.

Принципово можливі два варіанти вибору комп'ютерів для комп'ютерного блоку. З позиції уніфікації організації КС краще застосовувати два однотипні комп'ютери. Другий варіант полягає у застосуванні двох різних комп'ютерів. Внутрішній комп'ютер повинен бути більш продуктивним. Він не має безпосереднього доступу до Інтернету (зовнішнього світу), який можливий лише через зовнішній комп'ютер. Тому хакер, який територіально та юридично знаходиться поза межами КС, просто не має до нього доступу (проблема захисту від "ображеного співробітника", який знаходиться усередині КС, не розглядається). Зв'язок з Інтернетом для внутрішнього комп'ютера унеможливлюється програмним і апаратним шляхом.

Продуктивність зовнішнього комп'ютера, на який покладається функція зв'язку з Інтернетом (зовнішнім світом), не має бути великою. Крім приймання та передавання інформації, необхідної для розв'язання задачі, і зв'язку користувача з замовником та керівництвом, виконавець має змогу за необхідності використати зовнішній комп'ютер для власних потреб.

Зважаючи на недостатню захищеність зовнішнього комп'ютера, не можна виключити можливість того, що хакер зламає його систему захисту. Тому інформація, пов'язана з виробничою діяльністю фірми, має бути надійно криптозахищена і передаватися лише по захищених каналах зв'язку.

Для підвищення захищеності КС від вторгнення зв'язок між зовнішнім і внутрішнім комп'ютерами здійснюється через захисний екран, в якості якого застосовують універсальний чи спеціалізований комп'ютер або спецобчислювач (рис. 2).

Комп'ютерні блоки, які наведені на рис. 2, об'єднуються в територіально суміщену або територіально розподілену систему (мережу). На рис. 3 наведено приклад схеми захисту КС, яка містить п'ять робочих місць. Внутрішні комп'ютери об'єднані корпоративною мережею, зовнішні комп'ютери об'єднані за допомогою мережі Інтернет. На рис. 3 комп'ютерні засоби, з яких складається КС, розташовані у вигляді концентричних кіл, що нагадує обчислювальний пристрій середньовічного філософа та богослова Раймунда Луллія (Raymundus Lullius, 1235–1315), але кільцеве розташування комп'ютерних засобів у цьому випадку лише демонструє рівні захисту, які утворюються в КС внаслідок використання запропонованого підходу.

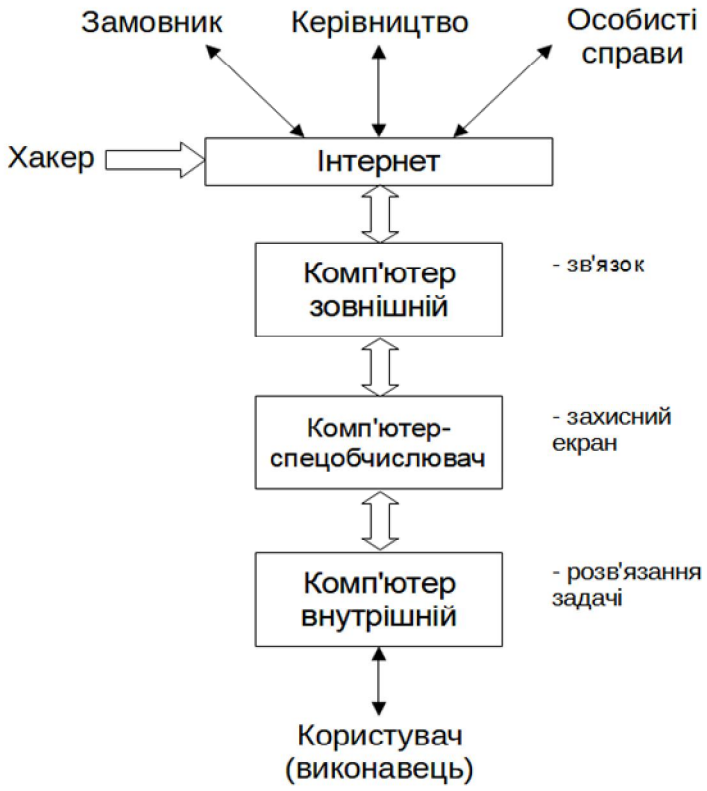

Рис. 2. Схема захисту КС від зовнішнього втручання шляхом апаратної надлишковості

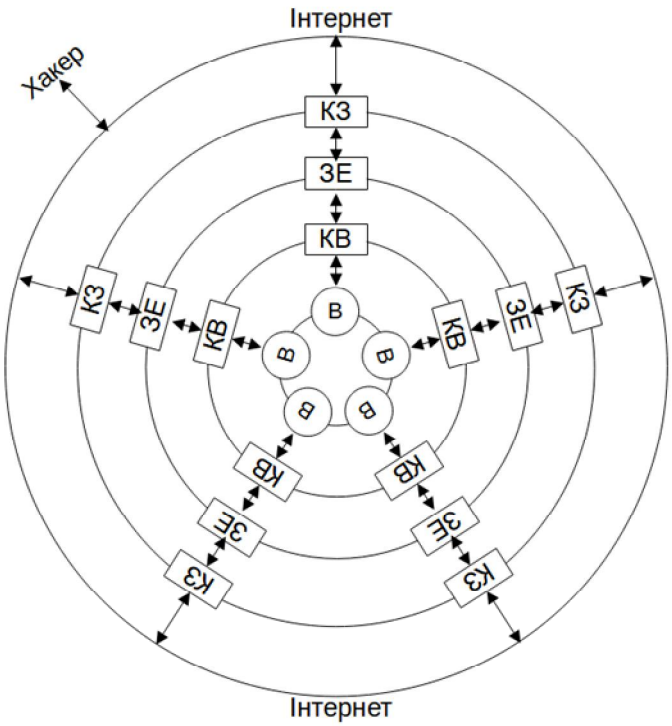

Рис. 3. Приклад схеми захисту КС із п'яти робочих місць, позначення: КВ – комп'ютер внутрішній, КЗ – комп'ютер зовнішній, ЗЕ – захисний екран, В – виконавець

4. Варіанти фізичного захисту КС

Поруч із застосуванням структурних методів, яким присвячена ця стаття, важливо пам'ятати про необхідність фізичного захисту КС. Зазначимо, що у найбільш складних з погляду існуючих загроз випадках КС повинна мати чотири контури фізичного захисту:

– зовнішній контур, який охоплює всю територію, де знаходяться технічні засоби КС;
– контур будівель та приміщень, в яких знаходяться технічні засоби КС;
– контур КС (апаратно-програмні засоби, елементи баз даних);
– контур технологічних процесів обробки інформації (введення/виведення, внутрішня комп'ютерна обробка тощо).

Як із гумором зауважив один американський фахівець: "Не кожен настільки удачливий, щоб використати для розташування обчислювального центру стару окружну в'язницю", що знаходиться, додав би автор статті, на острові, який оточують води океану.

Висновки

В статті розглянуто підхід до підвищення захищеності комп'ютерних систем від зовнішнього втручання. Обґрунтовано актуальність проблеми захисту інформації та кібербезпеки. Розглянуто стратегії нападу та деструктивних дій, які застосовують порушники (хакери). Виділено 16 різних стратегій нападу та порушень.

Проаналізовано причини вразливості комп'ютерних систем. Розглянуто дві групи причин: об'єктивні причини, які залежать від апаратно-програмних компонентів КС, та суб'єктивні причини, які залежать від людського фактору. Зазначено, що однією з основних причин, яка об'єктивно ускладнює захист комп'ютера від зовнішнього втручання, полягає в тому, що на один і той самий комп'ютер покладають розв'язання двох непов'язаних між собою проблем: безпосереднє розв'язання задачі, що, по суті, є внутрішньою проблемою, та здійснення зв'язку, що можна розглядати як зовнішню проблему.

Запропоновано підхід до підвищення захищеності комп'ютерних систем від зовнішнього втручання шляхом апаратної надлишковості, зокрема, замість одного комп'ютера застосовувати комп'ютерний блок, який складається з двох комп'ютерів – внутрішнього і зовнішнього. Внутрішній комп'ютер використовується для розв'язання задачі. На зовнішній комп'ютер покладається виконання функцій зв'язку. Додатково розглянуто питання фізичного захисту комп'ютерних систем.

Автор висловлює подяку президенту компанії SoftServe, канд. фізю-мат. наук Тарасу Володимировичу Кицмею за корисне обговорення проблеми захисту комп'ютерних систем від зовнішнього втручання.

Список літератури

1. Kianpour M.; Kowalski S.; Øverby H. (2021). Systematically Understanding Cybersecurity Economics: A Survey, Sustainability. 13 (24): 13677. – Pp. 1–28. DOI:10.3390/su132413677.

2. Santos J. C. S., Tarrit K., Mirakhorli M. (2017). A Catalog of Security Architecture Weaknesses, in Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA). – Pp. 220–223. DOI:10.1109/ICSAW.2017.25.

3. Deb R. & Roy S. (2022). A comprehensive survey of vulnerability and information security in SDN. Computer Networks. Vol. 206, 108802. – Pp. 1–21. DOI: 10.1016/j.comnet.2022.108802.

4. Williams P., Dutta I., Daoud H. & Bayoumi M. (2022). A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies. Internet of Things. 19. 100564. – Pp. 1–24. DOI:10.1016/j.iot. 2022.100564.

5. Bergh Johnsson D., Deogun D., Sawano D. (2019). Secure By Design, Manning Publications. – 410 p.

6. Xiaojuan M. (2017). Research and Implementation of Computer Data Security Management System. Procedia Engineering. Vol. 174. – Pp. 1371–1379. DOI: 10.1016/j.proeng.2017.01.290.

7. Morozova O., Nicheporuk A., Tetskyi A. & Tkachov V. (2021). Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks. Radioelectronic And Computer Systems. No. 4. – Pp. 145–156. DOI: 10.32620/reks.2021.4.12.

8. Gupta V., Singh S., Singh C. & Mangla A. (2022). A Systematic review on Cybersecurity: Models, Threats and Solutions, in Proceedings of the 10th International Conference on Emerging Trends in Engineering and Technology – Signal and Information Processing (ICETET-SIP-22). – Pp. 1–6. DOI: 10.1109/ICETET-SIP-2254415.2022.9791666.

9. Yemets V., Melnyk A., Popovych R. (2003). Modern cryptography. Basic concepts. Lviv: BaK. – 144 p. (in Ukrainian).

10. Villasenor J. (2010). The Hacker in Your Hardware: The Next Security Threat. Scientific American. 303 (2). – Pp. 82–88. DOI:10.1038/scientificamerican0810-82.

11. Neumann J. von. (2016). Probabilistic Logics and the Synthesis of Reliable Organisms From Unreliable Components, Automata Studies. (AM-34). Vol. 34, ed. by C. E. Shannon and J. McCarthy. Princeton: Princeton University Press. – Pp. 43–98. DOI: 10.1515/9781400882618-003.

12. Shannon C. E., Warren W. (1998). The Mathematical Theory of Communication. University of Illinois Press. – 144 p.

ABOUT ONE APPROACH TO INCREASING THE SECURITY OF COMPUTER SYSTEMS AGAINST INTRUSION

V. Golembo

Lviv Polytechnic National University,
Computer Engineering Department

The article considers an approach to increasing the security of computer systems from intrusion. The importance of the problem of information security and cybersecurity is substantiated. Strategies of attack and destructive actions used by intruders (hackers) are considered. 16 different attack and intrusion strategies are identified.

The reasons for the vulnerability of computer systems are analyzed. Two groups of reasons are considered: objective reasons depending on the hardware and software components of the computer system and subjective reasons depending on the human factor. It is noted that one of the main reasons that objectively complicate the protection of a computer from intrusion is that the same computer is assigned the solution of two unrelated problems: the direct solution of tasks, which are essentially an internal problem, and the tasks of communication, which can be seen as an external problem.

An approach is proposed to increase the security of computer systems from intrusion through hardware redundancy, in particular, instead of one computer, use a computer unit consisting of two computers – internal and external. The internal computer is used for the direct solution of tasks. The external computer is responsible for performing communication tasks. Additionally, the issues of physical protection of computer systems are considered.

Key words: information security, cybersecurity, intrusion.