https://doi.org/10.31891/2307-5732-2025-359-14
УДК 004.056.53:004.738.5

ГНАТЮК ВІКТОР
Державний університет «Київський авіаційний інститут»,
ДержНДІ технологій кібербезпеки
https://orcid.org/0000-0002-4916-7149
e-mail: viktor.hnatiuk@npp.kai.edu.ua
ЗАНДЕР КОСТЯНТИН
Державний університет «Київський авіаційний інститут»
https://orcid.org/0009-0006-4944-9249
e-mail: 8390983@stud.kai.edu.ua

МЕТОДИ ПІДВИЩЕННЯ ГАРАНТОВАНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ПРИКЛАДНИХ ІНТЕРНЕТ-СИСТЕМАХ

У статті розглянуто методи та модель підвищення гарантованості захисту персональних даних у прикладних Інтернет-системах на основі принципу транспарентності операційного середовища та публічного спостереження за діями адміністраторів у режимі реального часу. Запропоновано структуру операційного середовища з розмежуванням доменів безпеки, правила розмежування доступу, модель загроз і гарантії захисту, що відповідають вимогам нормативних документів України з технічного захисту інформації. Розроблена модель забезпечує підвищення довіри користувачів до сервісів та унеможливлює приховане порушення конфіденційності та цілісності даних під час їх обробки та передавання в Інтернет-середовищі.

Ключові слова: *персональні дані, технічний захист інформації, транспарентність, прикладні Інтернет-системи, модель загроз, гарантії захисту.*

GNATYUK VIKTOR
State University "Kyiv Aviation Institute"; ICTIP
ZANDER KOSTIANTYN
State University "Kyiv Aviation Institute"

METHODS OF INCREASING THE GUARANTEE OF PERSONAL DATA PROTECTION IN APPLIED INTERNET SYSTEMS

The article addresses the problem of ensuring a high level of assurance in the protection of personal data in application Internet systems, which are commonly implemented using a client-server architecture. Despite the availability of advanced information security subsystems, many users remain uncertain about the reliability of guarantees regarding the confidentiality and integrity of their personal data, particularly in critical application systems. This distrust is largely due to the lack of technical means that would allow clients to directly verify the actions of system administrators and to monitor the state of the operating environment during the provision of services.

The study proposes a model that combines the principle of transparency (operating environment openness) with public monitoring of all administrator activities in real time. The model is based on a logically structured operating environment divided into security domains, each with a clearly defined scope of permitted operations. Access control rules are developed to ensure strict isolation of personal data from any unauthorized access, while still enabling administrators to perform necessary maintenance without violating these restrictions.

A comprehensive threat model is formulated, focusing on scenarios that could compromise the confidentiality and integrity of personal data both within the server domain and in communication channels. The proposed security framework aligns with the Ukrainian national regulatory documents on technical information protection and includes a functional protection profile for client data that ensures maximum openness and controllability of the environment.

The results of the research demonstrate that implementing the proposed transparency-based model can significantly increase user trust, reduce the probability of undetected security breaches, and provide verifiable guarantees of personal data protection. The approach can be applied to various critical infrastructure systems and adapted to international cybersecurity standards. The proposed solutions can provide a level of protection sufficient to form the unquestionable trust of clients of Internet application systems.

Keywords: *personal data, technical information protection, transparency, application Internet systems, threat model, security assurance*.

Стаття надійшла до редакції / Received 03.10.2025
Прийнята до друку / Accepted 15.11.2025

Постановка проблеми

Захист персональних даних у прикладних Інтернет-системах залишається однією з ключових проблем сучасного інформаційного суспільства. Попри наявність розвинених підсистем технічного захисту інформації, користувачі не завжди впевнені у гарантованому збереженні конфіденційності та цілісності даних, особливо у критичних системах — електронного урядування, медичних сервісах, банківських платформах, хмарних сервісах.

Відсутність інструментів для постійного моніторингу дій адміністраторів та стану операційного середовища знижує рівень довіри. У клієнт-серверних архітектурах широкі привілеї адміністраторів створюють ризик несанкціонованого доступу до персональних даних без можливості оперативного виявлення.

Чинні моделі загроз та розмежування доступу часто не враховують, що джерелом ризику можуть бути самі адміністратори. Відсутність транспарентності та механізмів публічного спостереження у реальному часі підвищує ймовірність прихованих інцидентів.

Отже, необхідно розробити методи й моделі, що поєднують транспарентність, чітке розмежування доменів безпеки та контроль дій адміністраторів відповідно до національних нормативів ТЗІ та міжнародних стандартів кіберзахисту.

Аналіз останніх джерел

Питання забезпечення конфіденційності та цілісності персональних даних у прикладних Інтернет-системах досліджуються як в Україні, так і за кордоном. Класичні основи криптографії закладені К. Шенноном [2], який сформулював принципи секретних систем, та В. Діффі й М. Геллманом [4], що запропонували концепцію відкритого розподілу ключів. Подальший розвиток, зокрема алгоритмів на еліптичних кривих, відображено у стандарті ДСТУ 4145-2002 [3, 12].

Вітчизняні дослідження зосереджені на розробці моделей технічного захисту інформації відповідно до нормативних документів України у сфері ТЗІ [5, 6]. Вишняков та співавтори [1, 7] аналізували транспарентність і розмежування доступу в відкритих системах; Конахович і колектив авторів [9] — методи захисту в телекомунікаційних мережах із підвищеними вимогами безпеки. Напрацювання у галузі криптоаналізу [10] та використання безпечних ОС (наприклад, OpenBSD [8]) створюють базу для нових рішень.

Міжнародні стандарти та рекомендації (NIST SP 800-53 Rev.5, ISO/IEC 27701:2019, ENISA) підкреслюють важливість транспарентності — фіксації та аудиту всіх дій з персональними даними як засобу підвищення довіри та запобігання прихованим інцидентам.

Попри значну кількість досліджень, у тому числі [11-20], комплексна модель, що поєднує транспарентність, розмежування доменів безпеки та публічний моніторинг дій адміністраторів у реальному часі, досі не має повної реалізації.

Мета дослідження — створення методів та моделі підвищення гарантованості захисту персональних даних у прикладних Інтернет-системах шляхом інтеграції транспарентності операційного середовища, публічного моніторингу, розмежування доменів безпеки та правил доступу відповідно до національних і міжнародних стандартів.

Виклад основного матеріалу

Прикладні Інтернет-системи зазвичай будуються за архітектурою «клієнт/сервер», де існують ризики несанкціонованого доступу до серверних даних та порушення конфіденційності й цілісності інформації під час передавання через незахищені канали. Хоча сучасні підсистеми захисту часто відповідають вимогам власників, у критично важливих сервісах рівень гарантій захисту персональних даних залишається недостатнім.

Дослідження здійснюється задля створення умов, за яких порушення конфіденційності чи цілісності персональних даних клієнтів неможливе без їх відома, а будь-які спроби несанкціонованого доступу фіксуються без посередників. Для цього користувач повинен бути впевнений у ізоляції власних даних від сторонніх суб'єктів, зокрема адміністраторів, за винятком випадків, коли останні виконують необхідні технічні процедури (діагностика, відновлення, модернізація).

Щоб забезпечити довіру, розпорядник даних має мати змогу: перевіряти коректність усіх дій, пов'язаних зі створенням і налаштуванням операційного середовища від початку життєвого циклу системи до введення її в експлуатацію; безперервно спостерігати у реальному часі за діями адміністраторів у період надання послуг; бути впевненим, що в інші періоди (техобслуговування, модернізація) персональні дані повністю ізольовані навіть від адміністраторів.

Для підвищення гарантованості захисту операційне середовище повинно бути прозорим для клієнтів у частині дій адміністраторів. Перед запуском у робочий режим слід перевірити відсутність порушень у прийнятих правилах розмежування доступу (ПРД). Структура середовища має: забезпечувати логічну ізоляцію файлів з персональними даними від усіх користувачів, окрім клієнтів і адміністраторів; надавати адміністраторам технічну можливість роботи з усіма файлами, але із забороною використовувати її під час надання послуг; дозволяти клієнтам контролювати дотримання ПРД, зокрема перевіряти, чи адміністратори не отримують доступу до персональних даних у робочому режимі.

На рис. 1 наведено структуру операційного середовища транспарентної прикладної системи.

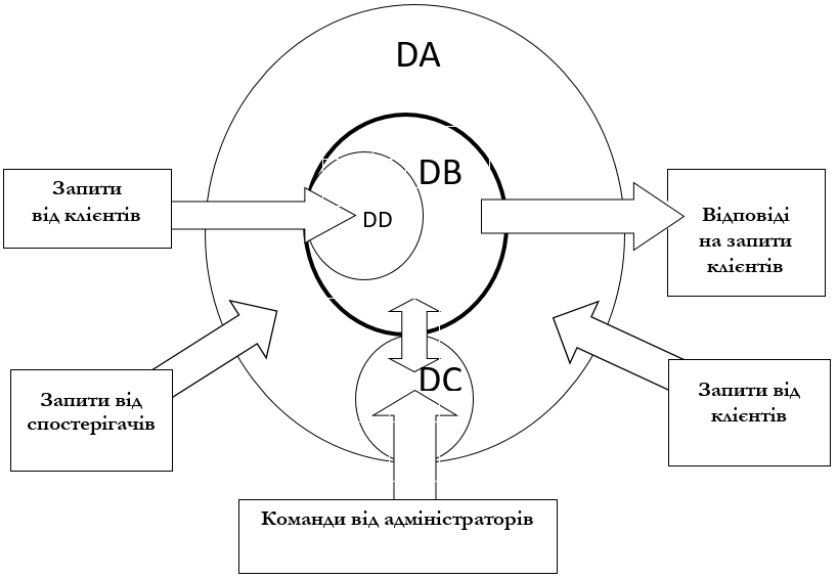

Рис.1. Структура транспарентної прикладної Інтернет-системи

Система складається з трьох доменів — DA, DB та DC, при цьому DB та DC розташовані всередині DA.

DA — зовнішній домен засобів спостереження за діями будь-яких суб'єктів, що намагаються отримати доступ до операційного середовища. Він забезпечує повний контроль процесів доступу та прозорість системи як для клієнтів, так і для сторонніх спостерігачів.

DB — внутрішній домен об'єктів захисту, зокрема файлів з персональними даними клієнтів. Порушення їх цілісності чи конфіденційності заборонено за будь-яких обставин, навіть адміністраторам. На схемі (рис. 1) він позначений суцільною лінією, що підкреслює його повну ізоляцію.

DC — внутрішній домен адміністраторів, який містить засоби інсталяції та управління системою, не пов'язані з об'єктами DB. У штатному режимі DC повністю ізольований від DB, а дії адміністраторів контролюються засобами з DA (переривчаста лінія на схемі).

Відповідно до п. 6.5 НД ТЗІ 1.1-002-99 [1], у такій структурі під час надання послуг адміністратори матимуть мінімальний рівень взаємодії з системою — лише запуск фіксованого набору програм, тоді як клієнти можуть самостійно переконатися у недоторканості своїх даних.

Правила розмежування доступу, що забезпечують ізольованість персональних даних та прозорість дій адміністраторів прикладної системи

Сформуємо ПРД для даної транспарентної системи.

Перш за все, зазначимо, що будь-який об'єкт доступу у прикладній системі входить до складу однієї із наступних п'яти множин:

- φ – множина файлів з персональними даними клієнтів;
- χ – множина відображень команд адміністраторів серверного обладнання, при чому $\chi \subset \phi$, $f: \chi \to \alpha$, де f – функція відображення;
- ψ – множина файлів у директорії, до якої має доступ адміністратор;
- ϑ – множина даних в оперативній пам'яті прикладної програми;
- ϕ – множина вихідних даних моніторингу звернень клієнтів, які прикладна програма використовує для авторизації цих клієнтів.

ПРД, що реалізуються засобами операційної системи (ОС) серверного обладнання прикладної системи, мають передбачати обмеження у діях над її об'єктами для наступних груп користувачів:

- α - множина усіх можливих дій (як штатних, так і позаштатних) адміністраторів серверного обладнання ІСВОД (припускається, що адміністратори можуть діяти на користь порушників ПРД);
- β - множина дій клієнтів прикладної системи під час їхніх звернень до цієї системи для обробки своїх персональних даних;
- γ - множина дій усіх інших суб'єктів доступу до оперативного середовища прикладної системи, що спостерігають за її функціонуванням з метою виявити факти порушення заданих ПРД (це можуть бути не тільки клієнти або контролюючі органи, але і будь-який із пересічних громадян, що бажає особисто упевнитись у відсутності будь-яких порушень конфіденційності та цілісності інформації у системі).

У транспарентній системі після виконання процедур налаштування мають підтримуватися наступні ПРД:

1. ОС серверного обладнання у режимі надання послуг має дозволяти виконувати тільки ті дії, які є елементами множини δ, де δ - об'єднання множин дій адміністраторів, клієнтів та спостерігачів системи, які в сукупності складають повну групу можливих дій будь-яких суб'єктів доступу до інформаційних ресурсів прикладної системи.

$$\delta = \alpha \cup \beta \cup \gamma. \tag{1}$$

Повна множина потенційних зловмисників та повна множина спостерігачів мають однакові права доступу, оскільки транспарентність системи передбачає можливість будь-якому суб'єкту спостерігати за її функціонуванням, будь-які інші дії, окрім спостереження, для потенційних зловмисників є забороненими.

2. Мають виконуватися наступні умови:

$$\psi \subset \phi;\ \vartheta \not\subset \phi;\ \varphi \subset \vartheta. \tag{2}$$

3. Дії адміністраторів прикладної системи над вище розглянутими об'єктами доступу мають не порушувати наступну умову

$$\alpha = W(\psi) \cup E(\psi), \tag{3}$$

де W – функція, що відповідає множині дій адміністратора для запису файлів (приєднання файлів до множини ψ); E – функція, що відповідає діям адміністратора щодо запуску програмних файлів на виконання (з множини ψ).

4. Дії клієнтів прикладної системи мають здійснюватися в межах дій, що відображаються наступним виразом:

$$\beta = \{G_1(f_M(\vartheta)), \ldots, G_i(f_M(\vartheta)), \ldots, G_n(f_M(\vartheta))\}, \tag{4}$$

де G_i – функція, що відповідає i-тому варіанту запиту клієнта $i = \overline{1,n}$; n – кількість варіантів запитів клієнта; f_M – функція моніторингу звернень клієнтів.

5. Дії спостерігачів прикладної системи мають здійснюватися в межах дій, що відображаються наступним виразом:

$$\gamma = R(\vartheta) \cup P, \tag{5}$$

де R– функція, що відповідає множині дій контролерів щодо ознайомлення з файлами множини ϕ, при чому $\chi \subset \vartheta, \psi \subset \vartheta$; P – множина дій спостерігача щодо отримання інформації від прикладної системи за допомогою команд ОС з метою виявлення можливих порушень політики безпеки.

На рис. 2 представлено схематичне відображення обмежень у правах доступу до ресурсів операційного середовища, що накладено на дії усіх можливих суб'єктів доступу, для того, щоб прикладну систему можливо було назвати транспарентною.

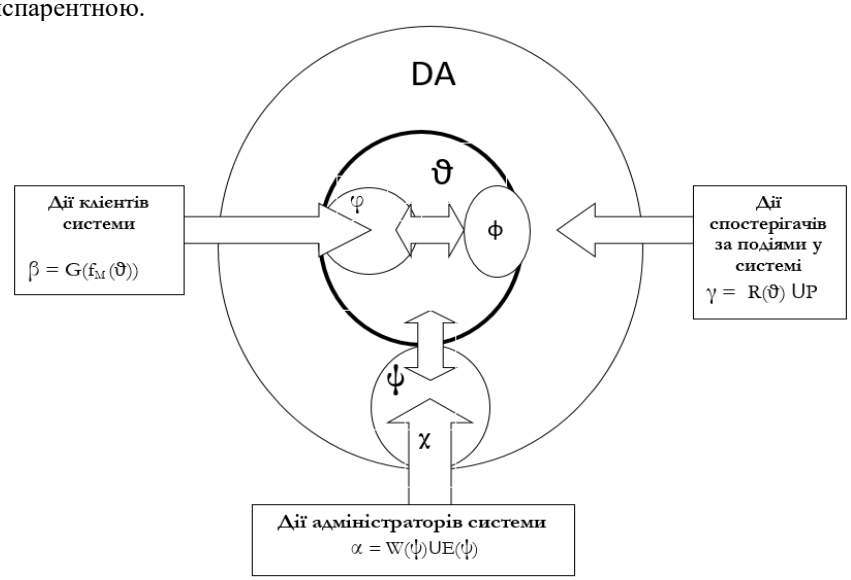

Рис. 2. Графічне відображення розподілу прав доступу груп суб'єктів до захищених об'єктів транспарентної прикладної Інтернет-системи

Транспарентність у цьому контексті означає неможливість здійснення несанкціонованих дій, які залишилися б непоміченими клієнтами системи. На схемі (рис. 2) кола та прямокутники позначають фізичну або логічну ізоляцію об'єктів. У межах зовнішнього кола — всі елементи операційного середовища, взаємодія яких має бути відкритою для спостереження. Водночас об'єкти з персональними даними ізолюються межами прямокутника φ і доступні лише власникам цих даних.

Згідно з прийнятими правилами розмежування доступу (ПРД), єдиними потенційними виконавцями несанкціонованих дій на серверному обладнанні є його адміністратори. Тому: адміністраторам дозволено лише дві операції — завантаження файлів у директорію системи та запуск з неї прикладних програм; клієнти мають можливість спостерігати всі дії адміністраторів, щоб виявити будь-які порушення.

Виконання цих вимог унеможливлює приховане втручання адміністраторів. Основна перевага транспарентних Інтернет-систем — можливість всеохоплюючого контролю з боку необмеженої кількості зацікавлених осіб, що гарантує цілісність і конфіденційність персональних даних.

Відповідно до НД ТЗІ 1.1-002-99 [2], усі автоматизовані системи, що працюють з інформацією з обмеженим доступом, повинні мати комплексну систему технічного захисту інформації (КСТЗІ), сертифіковану уповноваженим органом. Існуюча нормативна база України повністю охоплює захист підсистем управління, але персональні дані клієнтів прикладних систем не належать до таких підсистем. Тому визначення профілю їх захисту потребує окремого дослідження.

Далі розглядається множина загроз для клієнтських даних, що зберігаються на серверах або передаються каналами Інтернет під час надання послуг (табл. 1). Відсутність протидії цим загрозам підриває довіру до системи.

У таблиці 1 не враховано загрози, пов'язані зі змінами архітектури прикладної системи в періоди, коли вона не надає послуг клієнтам. Під час роботи системи потенційні ризики стосуються як системного, так і прикладного ПЗ, головно через помилки користувачів (перші сім загроз у табл. 1). Одним зі способів захисту є використання відкритого для публікацій ПЗ, що дозволяє сторонній аудит (підхід, обґрунтований [4]).

Однак навіть відкрите ПЗ може бути підмінене зловмисником. Для ускладнення НСД (несанкціонованого доступу) пропонується надати клієнтам можливість реального часу контролю всіх процесів і об'єктів у системі, а також засоби фіксації будь-яких відхилень від штатної роботи. ОС прикладної системи повинна: дозволяти інсталяцію та запуск ПЗ лише через штатні засоби ОС; забезпечувати безперервну роботу прикладних програм у режимі надання послуг; мати користувача-спостерігача з правом читання всіх файлів та виконання команд моніторингу адміністраторів; обмежувати адміністраторів лише копіюванням ПЗ у визначену директорію та запуском його; не містити користувача типу root.

Загрози включають: підміну прикладного ПЗ з подальшим відновленням оригіналу, якщо клієнт не фіксує послідовність дій адміністратора і не передбачено паузу між копіюванням та запуском; підміну сервера на фальшивий із синхронізацією журналів і метаданих, щоб приховати сліди. Запобігає цьому можливість клієнта запускати команду моніторингу процесів (наприклад, *ps aux* в OpenBSD) і порівнювати результати з початковими.

Таблиця 1

Множина загроз, що ставлять під сумнів конфіденційність та цілісність персональних даних клієнтів і можуть виникнути під час надання послуг клієнтам прикладної системи

№ з.п.	Визначення загрози	Шляхи протидії загрозі
1	Підміна штатного системного ПЗ прикладної системи іншим несанкціонованим позаштатним ПЗ	1. Використати відкрите для публікацій ПЗ 2. Використати структуру транспа-рентної прикладної Інтернет-системи із визначеними у підрозділі 2.2 ПРД, котра здатна гарантувати конфіденційність та цілісність персональних даних клієнтів в умовах недовіри до всіх без виключень процесів та осіб, що можуть мати доступ до ресурсів системи. 3. Використати метод спостереження у реальному часі за станом серверного обладнання і діями адміністраторів системи з боку необмеженого кола будь-яких користувачів Інтернету, що виключає можливість виникнення непомічених порушень прийнятої політики безпеки та усуває підстави для недовіри до коректної роботи системи.
2	Несанкціонована модифікація штатного системного ПЗ прикладної Інтернет-системи	
3	Несанкціонована модифікація штатного прикладного ПЗ	
4	Ініціація від імені адміністратора позаштатної команди управління у режимі надання послуг прикладною системою	
5	Фізична заміна елементів серверного обладнання	
6	Підміна відповідей на запити клієнтів	
7	Включення у склад серверного обладнання засобів реалізації атаки посередника	
8	Перехоплення та підміна автентифікаційних даних клієнта	Використати криптосемантичний метод досконало захищеного обміну даними, що гарантує цілісність та конфіденційність інформації при обміні даними через Інтернет.
9	Порушення конфіденційності та (або) цілісності даних, що просуваються каналами Інтернет	
10	Фізичний примус клієнта здійснити запит під контролем зловмисника	Використати метод нейтралізації спроб здійснення будь-яких видів тиску на клієнтів системи.

Підміну або модифікацію ОС унеможливлюють заходи згідно з НД ТЗІ 2.5-004-99.

Загрози підміни відповідей на запити клієнтів можуть виникати як на сервері, так і в каналах зв'язку (канальні атаки розглянуто в п. 2.5). При прозорій архітектурі та реалізації ПРД (п. 2.2) доступ до внутрішніх змінних прикладної програми зовнішнім суб'єктам заборонено, що знижує ризик серверної підміни.

Таким чином, серверне обладнання є головним проблемним доменом з точки зору НСД, а адміністратори — найбільш ймовірними порушниками ПРД. Таблиця 2 містить перелік їхніх можливих дій та методів протидії з боку клієнтів.

Таблиця 2

Несанкціоновані дії, які можуть бути реалізовані адміністраторами прикладної системи в домені серверного обладнання прикладної системи

Номер загрози	Опис можливих несанкціонованих дій адміністраторів прикладної системи	Метод протидії з боку клієнтів системи
1	Повна заміна ОС на серверному обладнання на іншу ОС, що має визначені зловмисником вразливості	Порівняння вмісту файлів ураженої ОС із змістом відкрито опублікованих файлів штатної ОС
2	Заміна окремих файлів штатної ОС або занесення нештатних додаткових файлів – джерел вразливостей	Порівняння каталогів і файлів інстальованої ОС із відкритими каталогами і файлами штатної ОС
3	Виконання позаштатної команди управління серверним обладнанням	Контроль за виконанням команд управління з боку клієнтів
4	Повна заміна прикладного ПЗ на інше, що має відповідні вразливості	Порівняння вмісту файлів ураженого прикладного ПЗ із змістом опублікованих файлів штатного прикладного ПЗ
5	Підміна окремих файлів прикладного ПЗ або його доповнення нештатними файлами – джерелами вразливостей	Контроль параметрів прикладного ПЗ шляхом виконання спеціальної команди виду *ps aux* в ОС *OpenBSD*
6	Доповнення штатної програми нештатними командами	Порівняння тексту програм з відомим штатним
7	Несвоєчасне виконання штатних дій	Перевірка дій за розкладом

Загроза атаки «людина посередині» (MITM) є однією з найнебезпечніших для прикладних систем критичного призначення. Її суть полягає в тому, що під час роботи системи клієнтам демонструється видимість нормального функціонування ОС, тоді як їхні запити непомітно перехоплюються та обробляються фальшивим сервером, який може змінювати або розкривати персональні дані.

Реалізація можлива через дії недобросовісних адміністраторів, які у два етапи підключають нештатні засоби за схемою, наведеною на рис. 3.

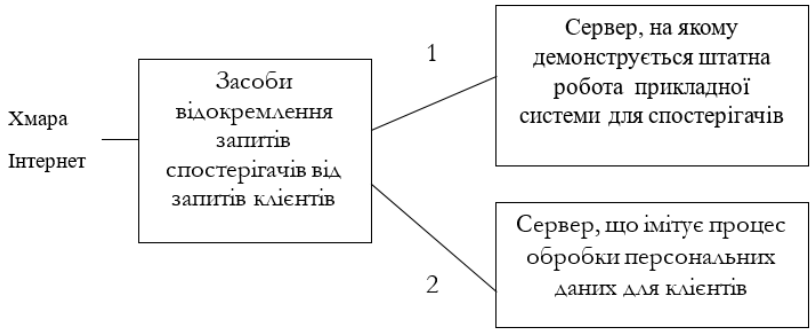

Рис. 3. Схема підключення обладнання для здійснення атаки посередника

Для протидії такій загрозі необхідно створити на сервері прикладної системи відкритий журнал обліку усіх запитів клієнтів [11]. Клієнт на початку сеансу зв'язку з сервером ВД має занести у відкритий журнал обліку запитів рядок з даними про час запиту разом з випадковим числом, що має бути сформоване на сервері. Виявлення Факт відсутності атаки *MITM* виявляється шляхом порівняння даних про момент часу запиту клієнта, котрий був зафіксований у журналі, із значенням випадкового числа. Таким чином кожен клієнт перед здійсненням акту запиту може самостійно впевнитись у тому, що він дійсно спілкується зі штатним сервером прикладної системи, а не з підробкою зловмисників.

Загрози перехоплення та підмін даних в каналах зв'язку

Крім протидії можливим несанкціонованим діям адміністраторів, які перелічені у табл.2.2, не менш важливо забезпечити захист від загроз ураження поза меж доменів безпеки серверного обладнання. Перелік можливих несанкціонованих дій зловмисників поза меж домену безпеки серверного обладнання разом з методами протидії цим діям представлено у табл. 3.

Таблиця 3

Несанкціоновані дії зловмисників поза меж домену безпеки серверного обладнання

Номер загрози	Опис НСД зловмисників	Метод протидії діям зловмисників
1	Перехоплення змісту запитів під час передавання	Створення захищеного каналу (криптографічний захист даних)
2	Заміна даних у запитах під час передавання	Використання протоколу, який забезпечує цілісність даних
3	Проникнення до серверу через засоби дистанційного доступу	Створення інтерфейсів, які від віддалених користувачів не сприймають нештатні запити
4	Заміна даних у відповідях на запити	Порівняння даних з довідками, отриманими через захищений канал

Виходячи з аналізу змісту табл. 3, мають підлягати захисту об'єкти та інформаційні потоки, що показані у табл. 4.

Таблиця 4

Інформаційні потоки та об'єкти, які потребують захисту у прикладній системі з метою протидії НСД до персональних даних клієнтів

Номер об'єкту	Опис об'єктів та процесів, що потребують захисту	Потрібна властивість КСЗІ
1	Потік даних від термінального обладнання клієнта до серверного обладнання прикладної системи	Забезпечення конфіденційності, цілісності та доступності
2	Потік даних від серверного обладнання до термінального обладнання клієнта прикладної системи	Забезпечення конфіденційності, цілісності та доступності
3	Команди адміністраторів з управління серверним обладнанням	Забезпечення цілісності та контрольованості
4	Файли, що завантажуються адміністратором на серверне обладнання	Забезпечення цілісності та контрольованості
5	Дані, що пов'язані зі процесом обробки запитів клієнтів	Забезпечення конфіденційності та цілісності
6	Усі без винятку файли на серверному обладнанні прикладної системи у реальному часі під час надання послуг клієнтам	Забезпечення цілісності та контрольованості

Загроза насильницького примусу клієнтів. Оскільки клієнт під час запиту перебуває поза межами доменів безпеки системи, існує ризик його примусу зловмисником виконати дію всупереч волі. Для протидії пропонується метод *імітаційного пароля*, коли система видає однакові на вигляд відповіді як на правильний пароль, так і на кілька спеціально підібраних хибних паролів. Це вводить зловмисника в оману, адже він не може відрізнити справжній результат від підробленого, навіть спостерігаючи за діями клієнта.

Модель захисту персональних даних. Побудова моделей захисту в АС від НСД регламентується НД ТЗІ та передбачає визначення функціональних профілів захищеності (ФПЗ) і гарантій їх реалізації.

– Функціональні послуги безпеки (ПБ) — набір нормативно визначених функцій, що протидіють загрозам; кожна ПБ має кілька рівнів досконалості.

– ФПЗ — перелік ПБ із заданими рівнями, здатними протистояти певній множині загроз.

– Гарантії — вимоги до розробки та експлуатації, що підтверджують коректність реалізації ФПЗ; існує 7 ієрархічних рівнів гарантій.

Для прикладних Інтернет-систем, що належать до класу 3, підкласу х.КЦ, стандартами НД ТЗІ 2.5-005-99 передбачено шість можливих ФПЗ, з яких слід обрати оптимальний залежно від призначення та умов роботи.

1) 3.КЦ.1 = {КД-2, КВ-1, ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1};

2) 3.КЦ.2 = {КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1, НВ-1};

3) 3.КЦ.3 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1};

4) 3.КЦ.4 = {КД-2, КА-2, КО-1, КК-1, КВ-3, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2};

5) 3.КЦ.5 = {КД-3, КА-3, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1};

6) 3.КЦ.6 = {КД-4, КА-4, КО-1, КК-2, КВ-4, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}.

Вибір ФПЗ для персональних даних клієнтів. Визначення ФПЗ для підсистем управління прикладними Інтернет-системами регламентовано НД ТЗІ 2.5-005-99 і не є предметом даного дослідження. Наше завдання — обрати ФПЗ для захисту персональних даних клієнтів.

Для досягнення мети — абсолютних гарантій захисту — необхідно забезпечити повний і безперервний контроль у реальному часі над усіма подіями, пов'язаними з обробкою, передаванням та зберіганням будь-яких файлів і процесів у системі. Модель захисту має надавати визначену множину послуг спостереження за діями осіб і процесів з правами адміністратора протягом усього часу роботи системи.

ФПЗ персональних даних повинен містити підмножину послуг безпеки (ПБ), що гарантують абсолютну відкритість та контрольованість середовища без зниження захисту підсистеми управління. Це означає повну реалізацію специфікацій як ФПЗ персональних даних, так і ФПЗ захисту від НСД до підсистеми керування.

Ключові вимоги до ПБ для контролю середовища: можливість спостереження за діями всіх об'єктів захисту та суб'єктів доступу; контроль у реальному часі будь-якими зацікавленими особами, незалежно від їхнього статусу чи прав; активні дії контролюючих осіб (не лише пасивне спостереження); відсутність обмежень на доступ до процедур контролю як основа довіри.

Функціональний профіль захищеності персональних даних клієнтів у прикладній системі наведено в табл. 5.

Таблиця 5

Функціональний профіль гарантованої для клієнтів захищеності персональних даних у прикладній системі, що функціонує в режимі надання послуг клієнтам

Назва процедури	**Сутність процедури та її виконавець**	**Назва послуги безпеки**	**Мнемоніка послуги безпеки**
Реєстрація клієнтів у прикладній системі	Занесення даних клієнтів у базу даних, клієнт/реєстратор	Ідентифікація та автентифікація отримувача	НП-1 НИ-1
	Введення пароля, претендент у клієнти	Ідентифікація та автентифікація відправника	НА-1 НИ-1
Підготовка серверного обладнання для роботи у режимі надання послуг клієнтам	Завантаження і запуск ОС, адміністратор	Коректність підтримки ФПЗ задаються критеріями гарантій (див. НД ТЗІ)	ФПЗ від НСД до підсистеми керування прикладною системою
	Завантаження і запуск прикладного ПЗ, адміністратор		
Ідентифікація та автентифікація клієнта, що генерує запит Створення захищеного каналу обміну даними	Введення ідентифікаційних та автентифікаційних даних, клієнт	Однонаправлений достовірний канал Одиночна ідентифікація та автентифікація	НК-1 НИ-2 Специфікація послуги криптосемантичного шифрування
	Введення пароля, клієнт		
	Шифрування запиту	Криптосемантичний захист	ФПЗ від НСД до підсистеми керування

Продовження таблиці 5

Приймання та обробка запита	Передавання даних від клієнта до сервера, клієнт	Ідентифікація і автентифікація при обміні Абсолютна конфіденційність при обміні	НВ-2 КВ-4
	Обробка запита, сервер	Один із шости можливих варіантів стандартних ФПЗ від НСД до підсистеми керування прикладною системою	ФПЗ від НСД до підсистеми керування прикладною системою
	Підготовка відповіді, сервер		
Вивід результатів обробки запита	Передавання даних від сервера до клієнта, сервер		
Спостереження за подіями в операційному середовищі прикладної системи, що функціонує в режимі надання послуг клієнтам	Перевірка на відсутність підмін та зловмисних модифікацій ОС та прикладного ПЗ, будь-який суб'єкт з правами спостерігача	Послуги публічного спостереження за операційним середовищем: 1) Аналіз в реальному часі; 2) Самотестування у реальному часі (за запитом спостерігача); 3) Розподіл обов'язків на підставі привілеїв; 4) Цілісність комплексу засобів захисту з функціями диспетчера доступу	НР-5 НТ-3 НО-3 НЦ-3
	Перевірка на відсутність підміни сервера, спостерігач		
	Контроль дій адміністраторів, спостерігач		

Синтез специфікацій послуг публічного спостереження (ППС). ППС включено до моделі захисту для забезпечення контролю операційного середовища прикладної системи необмеженим колом суб'єктів із правами спостерігачів. Відповідно до [НД ТЗІ 2.5-004-99], до складу ППС входять чотири стандартні послуги безпеки (ПБ) з найвищим рівнем спостереженості: НР-5 — Аналіз у реальному часі; НТ-3 — Самотестування у реальному часі (за запитом спостерігача); НО-3 — Розподіл обов'язків на підставі привілеїв; НЦ-3 — Цілісність комплексу засобів захисту (КЗЗ) з функціями диспетчера доступу.

Для кожної ПБ визначені окремі технічні вимоги до функціональності, журналювання, процедур тестування, ролей та політик безпеки.

Гарантії захисту персональних даних та коректності функціонування. Критерії гарантій рівня Г-7 передбачають транспарентність операційного середовища та відповідність [НД ТЗІ 2.5-004-99, пп. 10.1, 10.4]. Основні положення: повна відкритість штатного ПЗ та його специфікацій; використання апаратних засобів з відкритими стандартами; віддалений доступ до серверного обладнання через відкриті мережеві протоколи; неможливість модифікації або підміни ядра ОС у процесі надання послуг; можливість публічного контролю стану ОС, процесів і подій перезапуску.

Вимоги до відкритості та контрольованості: системне ПЗ (відкрите та просте для перевірок фахівцями з базовими знаннями ІТ; публікація специфікацій ОС в Інтернеті; заборона прихованих файлів; наявність команд для безперервного моніторингу роботи та процесів у реальному часі); прикладне ПЗ (відкрите, з публічними специфікаціями; шифрування персональних даних з практично неможливим дешифруванням у визначений термін; обробка конфіденційних даних лише в оперативній пам'яті; захист інтерфейсів від несанкціонованого доступу). Технологія обробки інформації: чітко регламентований порядок завантаження, запуску та управління; публічність розкладу роботи системи; можливість виявлення будь-яких відхилень від штатного режиму.

Висновки

У статті запропоновано модель операційного середовища прикладних Інтернет-систем із правилами розмежування доступу, що забезпечують клієнтам постійний контроль дій адміністраторів під час надання послуг. Структура реалізує принцип транспарентності та відповідає профілю захисту даних за НД ТЗІ, гарантує високий рівень захищеності та виявлення будь-яких несанкціонованих дій щодо персональних даних. Визначено умови забезпечення повної контрольованості середовища при нормативних рівнях ефективності та гарантованості захисту. Сформовано модель загроз, модель захисту, специфікації послуг публічного спостереження та гарантії безпеки персональних даних. Запропоновані рішення забезпечують рівень захисту, достатній для формування беззаперечної довіри клієнтів прикладних Інтернет-систем.

Література

1. Вишняков В. М. Відкрита система таємного голосування / В. М. Вишняков, М. П. Пригара, О. В. Воронін // Управління розвитком складних систем. – 2014. – № 20. – С. 110–115.

2. Shannon C. Communication Theory of Secrecy Systems / C. Shannon // Bell System Technical Journal. –

1949. – Vol. 28, No. 4. – P. 656–715.

3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Чинний від 01.07.2003.

4. Diffie W. New Direction in Cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. – 1976. – Vol. IT-22, No. 6. – P. 644–654.

5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний від 28.04.1999. – К. : ДСТСЗІ СБ України, 1999. – 14 с.

6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний від 28.04.1999. – К. : ДСТСЗІ СБ України, 1999. – 53 с.

7. Вишняков В. М. Захист даних в інформаційних системах : навч. посібник / В. М. Вишняков. – К. : КНУБА, 2009. – 128 с.

8. Fenollosa C. OpenBSD from a veteran Linux user perspective / C. Fenollosa. – 26.06.2015. – URL: http://cfenollosa.com/blog/openbsd-from-a-veteran-linux-user-perspective.html.

9. Конахович Г. Ф. Защита информации в телекоммуникационных системах / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов. – К. : МК-Пресс, 2005. – 279 с.

10. Сушко С. О. Математичні основи криптоаналізу : навч. посібник / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов ; Національний гірничий ун-т. – Д. : НГУ, 2010. – 465 с.

11. Core Technology Services. North Dakota University System, Grand Forks, ND 58201. – URL: https://listserv.nodak.edu.

12. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Чинний від 01.07.2003.

13. Alomar Saleh. Adaptive Method of Increase of Package Network Load / Saleh Alomar, Mhamad Alomar, V. M. Chuprin // International Journal of Engineering Science (IJES). – 2013. – Vol. 5. – P. 1006–1011. – URL: http://www.scirp.org/journal/eng. – DOI: 10.4236/eng.2013.512122. – ORCID iD: http://orcid.org/0000-0001-9412-7413.

14. Alomar Mhamad. Influence of traffic prognostic mechanism on quality of adaptive control of switchboard / Mhamad Alomar, Saleh Alomar, Atef Obeidat // International Journal of Engineering Science (IJES). – 2014. – Vol. 7, No. 33. – P. 1763–1776. – URL: http://www.scirp.org/journal/eng. – DOI: 10.12988/ces.2014.4797. – ORCID iD: http://orcid.org/0000-0001-9412-7413.

15. Альомар Мхамад. Прогнозування самоподібного трафіка у пакетних мережах / М. Альомар // Вісник КНУБА. Управління розвитком складних систем : зб. наук. праць. – 2014. – Вип. 20. – С. 102–109.

16. Альомар Мхамад Ібрагім Ахмад. Дослідження методу адаптивного управління портами пакетного комутатора / М. І. А. Альомар // Вісник КНУБА. Молодий вчений : зб. наук. праць. – 2014. – № 12. – С. 17–22.

17. Альомар Мхамад Ібрагім Ахмад. Збільшення корисного завантаження вузлового обладнання комп'ютерних мереж / М. І. А. Альомар // Вісник КНУБА. Управління розвитком складних систем : зб. наук. праць. – 2015. – Вип. 21. – С. 112–116.

18. Альомар Мхамад. Удосконалення технології управління розподілом ресурсів пакетних мереж / М. Альомар // Проблеми розвитку глобальних систем зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM : матеріали наук.-техн. конф. – К., 2012. – С. 45.

19. Вишняков В. М. Аналіз системних помилок адаптивного управління розподілом ресурсів мереж з комутацією пакетів / В. М. Вишняков, М. Альомар // Новітні комп'ютерні технології (NOCOTE'2012) : матеріали X Міжнар. наук.-техн. конф. – Севастополь, 2012. – С. 145–146.

20. Вишняков В. М. Збільшення корисного завантаження вузлового обладнання комп'ютерних мереж / В. М. Вишняков, М. Альомар // Новітні комп'ютерні технології (NOCOTE'2013) : матеріали XI Міжнар. наук.-техн. конф. – Кривий Ріг, 2013. – С. 159–160.

References

1. Vyshniakov V.M. Open system of secret voting / V.M. Vyshniakov, M.P. Pryhara, O.V. Voronin // Management of Complex Systems Development. - 2014. - No. 20. - P. 110-115.

2. Shannon C. Communication Theory of Secrecy Systems / C. Shannon // Bell System Technical Journal. - 1949. - Vol. 28, No. 4. - P. 656-715.

3. DSTU 4145-2002. Information technologies. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification. - Effective from 01.07.2003.

4. Diffie W. New Direction in Cryptography / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. - 1976. - Vol. IT-22, No. 6. - P. 644-654.

5. ND TZI 1.1-002-99. General provisions on information protection in computer systems against unauthorized access. - Effective from 28.04.1999. - Kyiv: DSSCSI SBU, 1999. - 14 p.

6. ND TZI 2.5-004-99. Criteria for evaluating information security in computer systems against unauthorized access. - Effective from 28.04.1999. - Kyiv: DSSCSI SBU, 1999. - 53 p.

7. Vyshniakov V.M. Data protection in information systems: textbook / V.M. Vyshniakov. - Kyiv: KNUBA, 2009. - 128 p.

8. Fenollosa C. OpenBSD from a veteran Linux user perspective / C. Fenollosa. - 26.06.2015. - URL: http://cfenollosa.com/blog/openbsd-from-a-veteran-linux-user-perspective.html.

9. Konakhovych H.F. Information protection in telecommunication systems / H.F. Konakhovych, V.P. Klimchuk, S.M. Рauк, V.H. Potapov. - Kyiv: MK-Press, 2005. - 279 p.

10. Sushko S.O. Mathematical foundations of cryptanalysis: textbook / S.O. Sushko, H.V. Kuznetsov, L.Ya. Fomychova, A.V. Korablov; National Mining University. - Dnipro: NGU, 2010. - 465 p.

11. Core Technology Services. North Dakota University System, Grand Forks, ND 58201. - URL: https://listserv.nodak.edu.

12. DSTU 4145-2002. Information technologies. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification. - Effective from 01.07.2003.

13. Alomar Saleh. Adaptive Method of Increase of Package Network Load / Saleh Alomar, Mhamad Alomar, V.M. Chuprin // International Journal of Engineering Science (IJES). - 2013. - Vol. 5. - P. 1006-1011. - URL: http://www.scirp.org/journal/eng. - DOI: 10.4236/eng.2013.512122. - ORCID iD: http://orcid.org/0000-0001-9412-7413.

14. Alomar Mhamad. Influence of traffic prognostic mechanism on quality of adaptive control of switchboard / Mhamad Alomar, Saleh Alomar, Atef Obeidat // International Journal of Engineering Science (IJES). - 2014. - Vol. 7, No. 33. - P. 1763-1776. - URL: http://www.scirp.org/journal/eng. - DOI: 10.12988/ces.2014.4797. - ORCID iD: http://orcid.org/0000-0001-9412-7413.

15. Alomar Mhamad. Forecasting of self-similar traffic in packet networks / M. Alomar // Bulletin of KNUBA. Management of Complex Systems Development: coll. sci. works. - 2014. - Iss. 20. - P. 102-109.

16. Alomar Mhamad Ibrahim Ahmad. Research of adaptive control method for packet switch ports / M.I.A. Alomar // Bulletin of KNUBA. Young Scientist: coll. sci. works. - 2014. - No. 12. - P. 17-22.

17. Alomar Mhamad Ibrahim Ahmad. Increasing useful load of node equipment in computer networks / M.I.A. Alomar // Bulletin of KNUBA. Management of Complex Systems Development: coll. sci. works. - 2015. - Iss. 21. - P. 112-116.

18. Alomar Mhamad. Improvement of resource distribution management technology in packet networks / M. Alomar // Problems of Development of Global Communication, Navigation, Surveillance and Air Traffic Management Systems CNS/ATM: proc. sci.-tech. conf. - Kyiv, 2012. - P. 45.

19. Vyshniakov V.M. Analysis of system errors in adaptive resource distribution management in packet-switched networks / V.M. Vyshniakov, M. Alomar // New Computer Technologies (NOCOTE'2012): proc. of 10th Int. sci.-tech. conf. - Sevastopol, 2012. - P. 145-146.

20. Vyshniakov V.M. Increasing useful load of node equipment in computer networks / V.M. Vyshniakov, M. Alomar // New Computer Technologies (NOCOTE'2013): proc. of 11th Int. sci.-tech. conf. - Kryvyi Rih, 2013. - P. 159-160.