DOI: 10.18372/2310-5461.66.20245
УДК 621.396

К. Ю. Зандер, PhD аспірант
Державний університет «Київський авіаційний інститут»
orcid.org/0009-0006-4944-9249
e-mail: 8390983@stud.kai.edu.ua;

В.О. Гнатюк, канд. техн. наук, доцент
Державний університет «Київський авіаційний інститут»
orcid.org/0000-0002-4916-7149
e-mail: viktor.hnatiuk@npp.kai.edu.ua

МЕТОД ПІДВИЩЕННЯ ГАРАНТОВАНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ПРИКЛАДНИХ ІНТЕРНЕТ-СИСТЕМАХ

Вступ

Прикладні інтернет-системи створюються, зазвичай, згідно з архітектурою «клієнт/сервер». Інформаційні ресурси таких систем зазнають загроз несанкціонованого доступу (НСД) до серверних даних, а також загроз, що пов'язані із порушеннями конфіденційності та цілісності даних під час їхнього транспортування через незахищені канали Інтернет. В таких системах наразі функціонують загалом досконалі підсистеми захисту інформації, які, в багатьох випадках, у цілому задовольняють потреби їхніх власників та користувачів. Але наявні підсистеми захисту, зазвичай, мають обмеження щодо довіри з боку користувачів. Зокрема, рівень гарантій захисту персональних даних у критично важливих системах не завжди відповідає очікуванням клієнтів. Тому мета даного дослідження полягає у розробці метода забезпечення гарантованої неможливості незафіксованого ураження персональних даних клієнтів, що зберігаються на серверах прикладної інтернет-системи та передаються через канали Інтернету.

Результати сучасних наукових досліджень в галузі інформаційної безпеки можуть слугувати основою для вирішення питань забезпечення гарантованості персональних даних у прикладних інтернет-системах. Однак в основу прийнятого підходу покладена концепція комплексної системи захисту інформації (КСЗІ) відповідно до положень діючих в Україні нормативних документів в галузі технічного захисту інформації (НД ТЗІ). Розгляд питань забезпечення гарантованості захисту в рамках інших більш перспективних концепцій інформаційної безпеки (мається на увазі різного роду ризик-орієнтовані підходи та моделі управління інформаційною безпекою з використанням стандартів *ISO/IEC* тощо) безумовно являє суттєвий науковий інтерес. Але в теперішніх реаліях України будь-які засоби та (або) технології захисту інформації, що призначені для використання в критично важливих застосуваннях, підлягають обов'язковій державній експертизі за критеріями ТЗІ. Даний метод розроблено виключно в межах чинної нормативної бази НД ТЗІ України, без претензії на узагальнення чи порівняння із сучасними міжнародними підходами, що дозволяє сподіватися на його застосування, не чекаючи завершення модернізації вітчизняної бази НД ТЗІ.

От же, згідно НД ТЗІ 2.5-03-99 в основі гарантованості захисту лежить беззаперечна віра клієнтів у те, що конфіденційність та (або) цілісність їхніх персональних даних ні за яких обставин не будуть порушені без їхнього відома. А будь-які спроби НСД до них будуть надійно зафіксовані особисто користувачами без додаткової участі будь-яких посередників. Користувачі мають бути упевнені, що файли з їхніми персональними даними є надійно ізольованими від впливу будь-яких інших суб'єктів або процесів, окрім них самих або їхніх довірених осіб. Для цього потрібно створити операційне середовище виконання комплексу прикладних програм, в якому така ізоляція буде забезпечена. Проте безумовна ізоляція файлів з персональними даними від впливу дій адміністраторів системи у загальному випадку не є доцільною, оскільки адміністратори за певних умов повинні мати можливість маніпулювання усіма елементами прикладної системи (зокрема, для контролю відповідності, діагностики, відновлення стану працездатності, модернізації, налагодження

параметрів тощо). Тому згідно даного методу необхідно, щоб розпорядник персональних даних (тобто, легальний клієнт прикладної системи) мав упевненість в неупереджених діях адміністраторів, він повинен мати можливість:

– перевірки коректності результатів усіх попередніх дій усіх суб'єктів, що мали відношення до створення та налагоджування операційного середовища прикладної системи на усіх етапах її життєвого циклу аж до моменту уведення її у режим надання послуг клієнтам;

– неперервного спостереження (моніторингу) за діями адміністраторів у реальному часі протягом усього періоду, коли система надає послуги своїм клієнтам.

Постановка проблеми

Для забезпечення гарантованості захисту необхідно, щоб розроблюваний метод передбачав реалізацію наступних функціональних можливостей. Можливість гарантування недоторканості персональних даних клієнтів (тобто, унеможливлення їхнього читання, копіювання, видалення та модифікації будь-яким несанкціонованим суб'єктом) шляхом створення відповідної структури операційного середовища прикладної інтернет-системи та відповідних правил розмежування доступу до нього. Можливість забезпечення повної контрольованості цього середовища з боку легальних клієнтів шляхом реалізації ідеї транспарентності, що передбачає побудову відповідного профілю захисту даних клієнтів. Цей профіль має підтримувати не тільки високі рівні захищеності персональних даних від порушень конфіденційності та цілісності, але і надавати можливість виявлення клієнтами будь-яких несанкціонованих дій, у т.ч. і з боку адміністраторів системи. Логіка взаємодії усіх елементів прикладної системи має гарантувати повну прозорість її технологічного циклу, забезпечувати в режимі надання послуг системою повну контрольованість з боку широкого загалу усіх дій адміністраторів системи.

От же, даний метод має забезпечити прозору архітектуру управління персональними даними клієнтів, що передбачає: 1) гарантовану недоторканість персональних даних шляхом чітко визначених правил розмежування доступу; 2) контрольованість операційного середовища клієнтами через механізми транспарентності та ведення профілів захисту; 3) можливість клієнтів самостійно виявляти несанкціоновані дії, зокрема з боку адміністраторів; 4) забезпечення прозорого технологічного циклу системи із механізмами реального моніторингу та аудиту дій адміністраторів.

Аналіз останніх досліджень та публікацій

Широке коло сучасних досліджень проблем інформаційної безпеки, зокрема в рамках *GDPR*, *NIST* SP 800-53, *ISO/IEC* 27001 та 27701, в той чи іншій мірі пов'язане з намаганнями підвищити гарантованість захисту інформації в прикладних інтернет-системах. Перш за все, слід вказати на публікації, що стосуються тематики транспарентності IT-систем, механізмів побудови довіри користувачів або сучасних моделей керування привілеями (наприклад, *Zero Trust Architecture*, принцип least privilege, моделі *PDP/PEP* тощо). Однак запропонований підхід не передбачає будь-яких аналізів ризиків, вразливостей, привілеїв чи інцидентів, оскільки основна мета даної роботи – досягнення абсолютної гарантованості захисту персональних даних шляхом застосування досконало стійких методів (зокрема, криптосемантичних, із збільшеною відстаню єдиності тощо) у транспарентному середовищі функціонування прикладних систем. Досконало стійкі методи захисту в межах своїх областей застосування роблять абсолютно неможливим будь-яке порушення конфіденційності персональних даних за будь-яких умов. Єдино можливий шлях забезпечення абсолютної гарантованості на формальному рівні – це поєднання результатів теорії досконалостійких систем з концепцією їхньої транспарентності. Тому пошук використаних джерел вівся на основі зіставлення двох ключових виразів – «досконало стійкі методи захисту інформації» та «транспарентні інформаційні системи». Мета такого пошуку – виявлення публікацій, де мова йде про використання досконало стійких методів захисту у транспарентних системах. У зв'язку з цим звернено увагу на публікації, де виконано порівняльний аналіз методів захисту інформації у сучасних телекомунікаціях, зокрема на роботи [1, 2]. Аналіз у цих роботах проведено за багатьма різнорідними критеріями, але, як виявилось, жоден із них не розглядав механізми, що забезпечують формальні гарантії інформаційної безпеки. У роботах [3–5] при побудові моделей захисту враховані параметри мережної безпеки, у тому числі параметри, що впливають на забезпечення гарантованої якості обслуговування. Проте шляхи забезпечення гарантій при застосування теоретично досконалих щодо стійкості систем захисту у цих роботах також не розглядаються. В роботі [6] синтез транспарентної телекомунікаційної структури здійснено на основі розв'язку оптимізаційної задачі, що пов'язана з різнотипними керуючими змінними. А кіберстійкість проектних рішень забезпечується тим, що у цільовій функції ураховуються показники мережної інформаційної безпеки, але параметри структури, що впливають на забезпечення гарантованої якості обслуговування,

не розглядаються як ті, що підлягають оптимізації. В якості прототипу щодо об'єкту даного дослідження можливо розглядати структуру, що представлена в роботі [7]. У цій роботі представлено схему та протокол інформаційної взаємодії елементів серверного обладнання, що функціонує у складі транспарентної прикладної інтернет-системи. Попри те, що в роботі [7] представлено загальні підходи до транспарентності інформаційних систем, запропонований підхід не передбачає розробки чітких правил розмежування доступу та функціонального профілю захисту персональних даних.

Таким чином, слід констатувати, що в наявних публікаціях проблема забезпечення абсолютної гарантованості захисту інформації в критично важливих прикладних застосуваннях висвітлена не у повній мірі. Так що розробка методу забезпечення гарантованої неможливості незафіксованого ураження персональних даних клієнтів прикладних інтернет-систем представляється актуальним завданням.

Виклад основного матеріалу

Щоб підвищити гарантованість захисту персональних даних у прикладній інтернет-системі, згідно даного методу її операційне середовище слід зробити прозорим (транспарентним) для клієнтів щодо дій адміністраторів цієї системи, а безпосередньо перед запуском її в режим надання послуг клієнтам слід здійснити ряд перевірок на відсутність будь-яких порушень у прийнятих правилах розмежування доступу (ПРД). У свою чергу, щоб забезпечити транспарентність системи, структура її операційного середовища має відображати логіку прийнятих обмежень в правах доступу усіх можливих груп користувачів до усіх створених об'єктів цього середовища. Названим вище вимогам відповідає структура операційного середовища транспарентної прикладної системи, що показана на рис. 1. Така структура в режимі надання послуг має забезпечувати:

1) логічну ізоляцію файлів з персональними даними клієнтів від усіх груп;

2) потенційних користувачів, окрім клієнтів та адміністраторів системи;

3) технічну можливість для адміністраторів маніпулювання усіма файлами;

системи, але із адміністративною забороною використання ними такої можливості у режимі надання послуг прикладної системи;

4) можливість спостереження з боку клієнтів за неухильністю виконання прийнятих ПРД, особливо можливість контролю дій адміністраторів системи, оскільки клієнтів слід забезпечити інструментом перевірки дотримання адміністраторами заборони щодо них доступу до персональних даних клієнтів у режимі надання послуг користувачам.

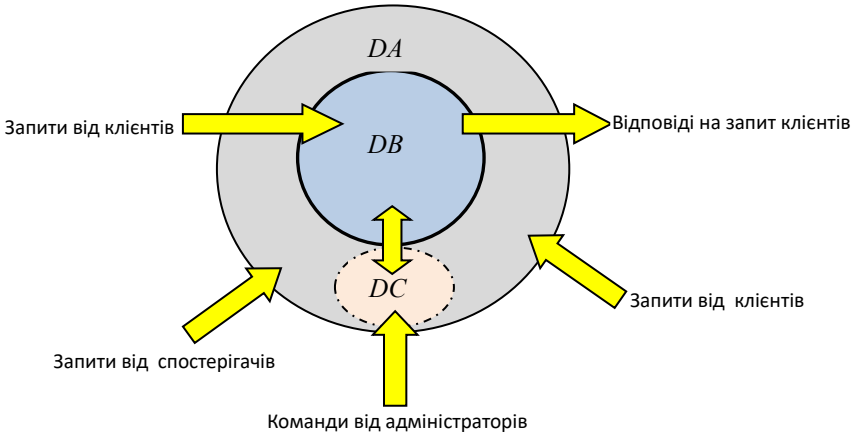

Рис. 1. Структура транспарентної прикладної інтернет-системи

Як бачимо, даний метод побудови операційного середовища прикладної системи передбачає, що структура цього середовища складається із трьох доменів – *DA, DB* та *DC*. При цьому домени *DB* та *DC* знаходяться всередині домену *DA*. Зовнішній домен DA – це домен засобів спостереження за діями будь-яких суб'єктів, що намагаються отримати доступ до операційного середовища прикладної системи. Ці засоби спостереження призначені для забезпечення повного контролю усіх процесів доступу до операційного середовища системи. Тим самим забезпечується прозорість системи не тільки з боку клієнтів системи, але і з боку будь-яких інших пересічних громадян. Внутрішній домен *DB* – це домен об'єктів захисту (у т.ч., файлів з персональними даними клієнтів), порушення цілісності та конфіденційності котрих не припускається ні за яких обставин. Таке не дозволяється нікому, навіть адміністраторам з найвищими рівнями повноважень. Домен *DB* на

рис. 1. відокремлюється від усіх інших елементів операційного середовища суцільною лінією, що вказує на повну ізольованість його внутрішніх об'єктів. Внутрішній домен *DC* – це домен адміністраторів системи. У ньому містяться засоби початкової інсталяції та адміністрування, що не мають відношення до об'єктів домену *DB*. Тобто, у штатному режимі надання послуг засоби домену *DC* абсолютно ізольовані від об'єктів домену *DB*. Так що адміністратори не можуть впливати на процеси в домені *DB*. У той же час робота засобів адміністрування може контролюватися засобами спостереження із домену *DA*, що відображається на рис. 1. переривчатою лінією навколо домену *DC*.

Якщо структура операційного середовища прикладної системи буде відповідати зазначеним вище умовам, то у режимі надання послуг її адміністратори згідно п.6.5 НД ТЗІ 1.1-002-99 [1] будуть мати найнижчий рівень можливостей проведення діалогу з прикладною системою (тільки можливість запуску фіксованого набору програм, що реалізують заздалегідь передбачені функції обробки інформації) у той час, як її клієнти зможуть самостійно упевнитись у недоторканості своїх персональних даних.

У рамках даного методу, необхідно сформувати правила розмежування доступу (ПРД), що забезпечують ізольованість персональних даних та прозорість дій адміністраторів для даної транспарентної прикладної 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 прикладної системи (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).

От же, даний метод передбачає, що транспарентна система після виконання процедур налаштування буде здатна підтримувати 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.

$$\delta = \alpha \cup \beta \cup \gamma. \qquad (1)$$

2. Мають виконуватися наступні умови:

$$\Psi \subset \phi; \ \vartheta \not\subset \phi; \ \varphi \subset \vartheta. \qquad (2)$$

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

$$\alpha = W(\Psi) \cup E(\Psi), \qquad (3)$$

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:

$$\beta = \{G_1(f_M(\vartheta)),...,G_i(f_M(\vartheta)),...,G_n(f_M(\vartheta))\}, \qquad (4)$$

де G_i – функція, що відповідає і-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:

$$\gamma = R(\vartheta) \cup P \qquad (5)$$

де R – функція, що відповідає множині дій контролерів щодо ознайомлення з файлами множини ϕ, при чому $\chi \subset \phi$; 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. Транспарентність у даному випадку означає неможливість здійснення будь-яких несанкціонованих дій, які б не були виявлені клієнтами прикладної системи.

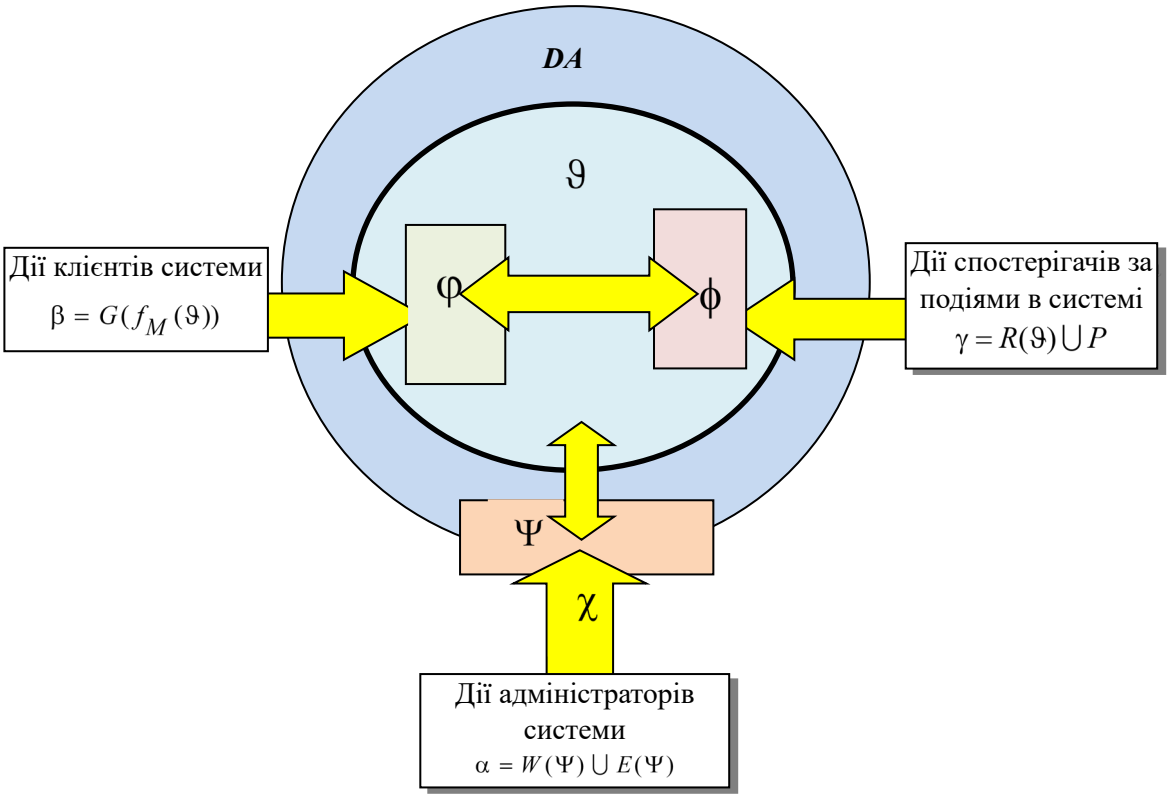

Рис. 2. Графічне відображення розподілу прав доступу груп суб'єктів до захищених об'єктів транспарентної прикладної інтернет-системи

Лінії кіл та прямокутників, відображених на рис. 2 означають фізичну або логічну ізоляцію об'єктів, що знаходяться у середині цих кіл або прямокутників. Зокрема все, що знаходиться у середині зовнішнього кола, це елементи операційного середовища прикладної системи – об'єкти та процеси, що взаємодіють між собою під час функціонування цієї системи. Відповідно до принципу транспарентності операційне середовище має бути прозорим, тобто доступним для спостереження з боку широкого загалу. У той же час множина об'єктів, що містять персональні дані клієнтів, мають бути недоступними для будь-яких суб'єктів, окрім власників цих даних. Тому ці об'єкти ізольовані межами прямокутника ϕ.

Інші об'єкти захисту в операційному середовищі також ізолюються межами внутрішніх кіл та прямокутників (як від зовнішнього середовища, так і від певних категорій користувачів) відповідно до прийнятих ПРД.

От же, даними ПРД передбачено, що єдиними користувачами, які, у принципі, мають можливість виконувати несанкціоновані дій на серверному обладнанні, є адміністратори цього обладнання. Будь-які дії інших користувачів – клієнтів та спостерігачів - не у змозі створити загрозу штатній роботі обладнання у режимі надання послуг клієнтам системою. Тому є принциповим, щоб будь-яку нештатну дію адміністраторів могли виявити клієнти і будь-які інші суб'єкти, що зацікавлені в ефективній роботі підсистеми захисту персональних даних клієнтів. Ця принципова умова згідно даного методу досягається шляхом реалізації наступних двох правил. По-перше, для запобігання можливим несанкціонованим діям адміністраторів цими ПРД адміністраторам системи дозволено виконувати лише дві дії, а саме, заносити файли у її директорію і запускати на виконання прикладну програму лише з цієї директорії. Під час надання послуг клієнтам системою усі інші дії адміністраторам заборонено. По-друге, у системі має бути реалізована послуга спостереження за

усіма діями адміністраторів з боку клієнтів системи для того, щоб будь-яку нештатну дію адміністраторів могли виявити клієнти. Якщо задані вище ПРД будуть реалізовані на практиці, то адміністратори не зможуть здійснити дії щодо управління прикладною системою, які можна було б приховати від спостерігачів.

Даний метод дозволяє реалізувати головну перевагу транспарентних прикладних інтернет-систем – можливість їх всеохоплюючого контролю з боку необмеженої кількості будь-яких зацікавлених осіб, оскільки тільки такий контроль гарантує клієнтам конфіденційність та цілісність їхніх персональних даних.

Щодо шляхів реалізації методу слід зазначити, що відповідно до положень Служби з питань технічного захисту інформації Служби Безпеки України (СТЗІ СБУ) НД ТЗІ 1.1-002-99 будь-які автоматизовані системи (у т.ч. і прикладні інтернет-системи), що призначені для обробки інформації з обмеженим доступом, мають містити у своєму складі штатну комплексну систему технічного захисту інформації (КСТЗІ), яка пройшла експертизу уповноваженим органом на відповідність нормативним документам України у сфері ТЗІ (НД ТЗІ). Існуюча нормативна база України у сфері ТЗІ є функціонально повною щодо забезпечення захисту від несанкціонованого доступу (НСД) саме для підсистем управління автоматизованими системами. Тому рівень формалізації викладу даного матеріалу обрано з урахуванням вимог НД ТЗІ. Цей виклад обрано на мові специфікацій функціональних послуг безпеки, що надана у чинному НД ТЗІ 2.5-004-99 (у редакції 2012 року).

Специфікації послуг безпеки, що відображені у НД ТЗІ України, відповідно до НД ТЗІ 2.5-004-99 дозволяють визначити функціональні профілі захисту інформації саме для таких підсистем. Проте персональні дані клієнтів, що зберігаються у файлах прикладних систем та (або) циркулюють каналами Інтернет, не є елементами підсистем управління і, от же, можливість визначення профілю їхнього захисту у термінах специфікованих послуг безпеки (ПБ) підлягає окремому дослідженню.

Реалізація методу передбачає необхідність розгляду множини загроз для персональних клієнтських даних, що зберігаються у файлах на серверах інтернет-системи. Зазначимо тільки ті загрози, що можуть мати місце під час надання послуг системою. Цю множину специфічних загроз, що ставлять під сумнів конфіденційність та цілісність персональних даних клієнтів, представлено у табл. 1. Зрозуміло, що відсутність протидії цим загрозам буде підривати довіру клієнтів щодо гарантій захисту їхніх персональних даних.

Таблиця 1

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

<table>
<tr><th>№ з.п.</th><th>Визначення загрози</th><th>Шляхи протидії загрозі</th></tr>
<tr><td>1</td><td>Підміна штатного системного ПЗ прикладної системи іншим несанкціонованим позаштатним ПЗ</td><td rowspan="7">1. Використати відкрите для публікацій ПЗ.
2. Використати структуру транспа-рентної прикладної інтернет-системи із визначеними 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.</td></tr>
<tr><td>2</td><td>Несанкціонована модифікація штатного системного ПЗ прикладної інтернет-системи</td></tr>
<tr><td>3</td><td>Несанкціонована модифікація штатного прикладного ПЗ</td></tr>
<tr><td>4</td><td>Ініціація від імені адміністратора позаштатної команди управління у режимі надання послуг прикладною системою</td></tr>
<tr><td>5</td><td>Фізична заміна елементів серверного обладнання</td></tr>
<tr><td>6</td><td>Підміна відповідей на запити клієнтів</td></tr>
<tr><td>7</td><td>Включення у склад серверного обладнання засобів реалізації атаки посередника</td></tr>
<tr><td>8</td><td>Перехоплення та підміна автентифікаційних даних клієнта</td><td rowspan="2">Використати криптосемантичний метод досконало захищеного обміну даними, що гарантує цілісність та конфіденційність інформації при обміні даними через Інтернет.</td></tr>
<tr><td>9</td><td>Порушення конфіденційності та (або) цілісності даних, що просуваються каналами Інтернет</td></tr>
<tr><td>10</td><td>Фізичний примус клієнта здійснити запит під контролем зловмисника</td><td>Використати метод нейтралізації спроб здійснення будь-яких видів тиску на клієнтів системи.</td></tr>
</table>

Модель захисту персональних даних у прикладній системі згідно даного методу має будуватися з урахуванням даних табл. 1 і відповідати вимогам, що викладені нижче.

Побудова моделей захисту інформації в автоматичній системі (АС) від НСД має регламентуватися положеннями вітчизняних НД ТЗІ [1.1-002-99, 1.1-003-99, 2.5-004-99, 2.5-005-99]. Результатом такої побудови мають бути відповідним чином визначені функціональні профілі захищеності (ФПЗ) оброблюваної у них інформації від НСД та специфікації гарантій такого захисту.

Слід зазначити, що з точки зору ТЗІ підсистема захисту інформації будь-якої АС розглядається як така, що надає певний набір функціональних послуг безпеки (ПБ), котрі у сукупності мають домірно протидіяти можливостям реалізації тій множині загроз, що у даних конкретних умовах використання АС вважаються суттєвими. Кожна ПБ реалізує нормативно визначений набір функцій, що дозволяє протистояти деякій підмножині суттєвих загроз. У свою чергу, кожна ПБ згідно НД ТЗІ 2.5-004-99 може включати декілька рівнів досконалості (стійкості або потужності). Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз.

Семантичні позначення ПБ та їхні специфікації надані у НД ТЗІ 2.5-005-99. ФПЗ являє собою перелік ПБ із визначеними для них рівнями, реалізація котрих у складі АС забезпечує протидію заданій множині загроз із заданим рівнем гарантованості такого захисту. Критерії гарантій дозволяють оцінити коректність реалізації ФПЗ і представляють собою специфіковані вимоги до різних аспектів створення та функціонування підсистеми захисту інформації в АС на різних етапах її життєвого циклу. В НД ТЗІ 2.5-004-99 специфіковано сім рівнів гарантій, які є ієрархічними. Чим вище рівень гарантій, тим більша міра упевненості в тому, що ФПЗ коректно обраний щодо протидії визначеній множині загроз і може забезпечити очікуваний споживачами рівень захищеності інформації під час експлуатації АС.

От же, даний метод передбачає необхідність визначення ФПЗ та гарантій забезпечення захисту персональних даних клієнтів прикладної інтернет-системи.

Слід розрізняти ФПЗ для підсистем управління прикладною інтернет-системою від ФПЗ персональних даних клієнтів цієї системи.

У [НД ТЗІ 2.5-005-99] надано класифікацію АС та стандартні ФПЗ у розрізі кожного класу АС саме для підсистем управління. Прикладні інтернет-системи відносяться до класу 3 (розподілені багатомашинні багато користувачеві комплекси, які оброблюють інформацію різних категорій конфіденційності). У рамках класу 3 вони відносяться до підкласу х.КЦ (АС, до яких пред'являються підвищені вимоги щодо забезпечення конфіденційності та цілісності оброблюваної інформації). В залежності від призначення прикладної системи та конкретних умов її функціонування доцільно обрати один із наступних шістьох стандартних ФПЗ:

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}.

Семантика ФПЗ визначена у п.6.2 НД ТЗІ 2.5-005-99, а рекомендації щодо вибору ФПЗ – у Додатку А цього ж документу).

Так що визначення ФПЗ для підсистем управління прикладними інтернет-системами не являє наукове завдання і, от же, у даній роботі не розглядається. Треба лише визначити умови функціонування конкретної прикладної системи і обґрунтувати вибір одного із представлених вище стандартних ФПЗ.

Для досягнення заявленої мети даної роботи, а саме, забезпечення абсолютних гарантій захисту персональних даних у прикладній системі, необхідно надати можливість широкому загалу (і, перш за все, клієнтам системи) повного і безперервного контролю у реальному часі подій, що пов'язані з обробкою, транспортуванням та збереженням усіх без винятку файлів і процесів, що функціонують у цій системі. От же, модель захисту має передбачати надання пересічним громадянам та зацікавленим організаціям певним чином визначеної множини послуг спостереження за усіма діями осіб та процесів з правами адміністраторів протягом усього часу, коли прикладна система знаходиться у режимі надання послуг клієнтам.

Даний метод передбачає, що функціональний профіль захисту [НД ТЗІ 2.5-004-99] персональних даних клієнтів містить у своєму складі, поряд з іншим, підмножину послуг безпеки (ПБ), що забезпечують абсолютну (повну) відкритість та контрольованість середовища функціонування цієї системи.

Слід підкреслити, що забезпечення відкритості та контрольованості операційного середовища має не зменшувати ефективність та гарантованість захисту від НСД до підсистеми керування прикладною системою. Це означає, що модель захисту прикладної системи має у повній мірі реалізовувати специфікації як ФПЗ персональних даних клієнтів, так і ФПЗ від НСД до підсистеми керування прикладною системою.

Специфікації ПБ, що забезпечують контрольованість середовища, мають відображати не тільки особливості реалізації функцій спостереження за подіями в операційному середовищі, але і забезпечувати можливість контролю дій усіх без винятку об'єктів захисту та суб'єктів доступу з боку будь-яких без винятку зацікавлених осіб у реальному часі функціонування прикладної системи. Такий контроль не є пасивним спостереженням, а передбачає активні дії суб'єктів, незалежно від їхнього статусу та прав доступу. Клієнти тільки тоді будуть мати беззаперечну довіру до наданих гарантій щодо захисту їхніх персональних даних, коли буде організована ефективна протидія несанкціонованим діям з боку будь-яких осіб з будь-якими правами доступу, а функції контролю можуть здійснювати будь-які зацікавлені особи. Відсутність обмежень у доступі до процедур контролю є основною умовою забезпечення гарантій. Таким чином функціональний профіль гарантованої для клієнтів захищеності персональних даних у прикладній системі, що функціонує у режимі надання послуг клієнтам можна надати у вигляді табл. 2.

Таблиця 2

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 автен-тифікація 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	Введення ідентифікаційних та автентифікаційних даних, клієнт	Однонаправлений достовірний канал	НК-1 НИ-2
Створення захищеного каналу обміну даними	Введення пароля, клієнт	Одиночна ідентифікація та автентифікація	Специфікація послуги криптосемантичного шифрування
	Шифрування запиту	Криптосемантичний захист	ФПЗ від НСД до підсистеми керування
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 запиту, сервер	Один із шести можливих варіантів стандартних ФПЗ від НСД до підсистеми керування прикладною системою	ФПЗ від НСД до підсистеми керування прикладною системою
	Підготовка відповіді, сервер		

Закінчення табл. 2

Назва процедури	Сутність процедури та її виконавець	Назва послуги безпеки	Мнемоніка послуги безпеки
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 с ередовищем: 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		

Висновки

1. Запропоновано метод забезпечення гарантованості захисту персональних даних клієнтів прикладних систем. Згідно даного методу модель структури операційного середовища обробки запитів для прикладних інтернет-систем реалізує ідею транспарентності та відтворює згідно НД ТЗІ 2.5-005-99 профіль захисту даних клієнтів, що забезпечує не тільки високі рівні захищеності цих даних, але і можливість для клієнтів виявлення будь-яких несанкціонованих дій щодо їхніх персональних даних. Синтезовано відповідні правила розмежування доступу (ПРД), що забезпечують клієнтам можливість контролю дій адміністраторів системи упродовж усього часу, коли система надає послуги своїм клієнтам.

2. У цілому характеристики розробленої структури, ПРД, моделі загроз, моделі захисту, а також специфікацій гарантій такого захисту дозволяють зробити висновок, що у випадку практичної реалізації названих вище доробок досягнутий рівень гарантованості захисту буде достатнім, щоб сподіватися на беззаперечну довіру клієнтів прикладних інтернет-систем щодо гарантій захисту їхніх персональних даних.

ЛІТЕРАТУРА

[1] Котляров О. Ю., Бортнік Л. Л. Порівняльний аналіз систем захисту у телекомунікаційних мережах. *Сучасний захист інформації*. № 4 (60), 2024. С. 60–72.

[2] Dordal P. L. An Introduction to Computer Networks. Loyola University Chicago, Department of Computer Science, 2020. 872 p.

[3] Добровольський Є. В., Нечипорук О. Л. Моделювання мережевого трафіку з використанням контекстних методів. *Наукові праці ОНАЗ ім. О. С. Попова*. 2005. № 1. С. 24–32.

[4] Lemeshko O., Shapovalova A., Al-Dulaimi A., Yeremenko O., Yevdokimov. A Flow-Based Routing Model with Load Balancing Considering Network Security Parameters // Scientific Journal of NTUU "Igor Sikorsky Kyiv Polytechnic Institute" «Information and Telecommunication Sciences». № 2, 2020. С. 44–60.

[5] Лемешко О., Єременко О., Євдокименко М., Батул Слейман. Оптимізація процесів забезпечення гарантованої якості обслуговування та мережної безпеки під час маршрутизації шляхами, що не перетинаються. Науковий журнал НТУУ «Київський політехнічний інститут імені І. Сікорського» «*Information and Telecommunication Sciences*». № 2, 2023. С. 33–39.

[6] Лемешко О. В., Єременко О. С., Куренко В. О., Фукс М. А. Метод проєктування кіберстійкої інфокомунікаційної мережі. Проблеми телекомунікацій. № 2 (35), 2024. С. 14–25.

[7] Мачалін І. О., Комарницький О. О., Гнатюк В. О. Удосконалення технології доступу до ресурсів транспарентних систем Інтернет-голосування. *Наукоємні технології*. № 4 (40), 2018. С. 415–423.

Зандер К. Ю., Гнатюк В. О.

МЕТОДИ ПІДВИЩЕННЯ ГАРАНТОВАНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ПРИКЛАДНИХ ІНТЕРНЕТ-СИСТЕМАХ

Існуючі технології захисту операційного середовища прикладних систем не забезпечують повного захисту від несанкціонованих дій адміністраторів із найвищими рівнями повноважень, оскільки не гарантують повної контрольованості процесів у цих середовищах. Це знижує довіру користувачів до гарантованого захисту їхніх персональних даних.

Єдиним ефективним способом захисту операційного середовища від зовнішніх загроз є його повна ізоляція. Для критично важливих прикладних застосувань вона має відповідати гарантійним критеріям НД ТЗІ 2.5-004-99 на рівні Г-7. При цьому необхідно забезпечити повну контрольованість ізоляції, що можливо лише в інтернет-системах із транспарентним програмно-апаратним середовищем.

Запропоновано, щоб структура прикладних систем критичного призначення була транспарентною, а функціональний профіль захисту (ФПЗ) включав послугу спостереженості згідно з НД ТЗІ 2.5-004-99. Гарантії коректності реалізації цієї функціональності на рівні Г-7 є ключовим фактором довіри клієнтів до системи. Також обґрунтовано використання методів теоретично досконалого захисту, що забезпечують абсолютну стійкість щодо порушень конфіденційності даних за певних умов. Синтезовано відповідні правила розмежування доступу (ПРД), що забезпечують клієнтам можливість контролю дій адміністраторів системи упродовж усього часу, коли система надає послуги своїм клієнтам. У цілому характеристики розробленої структури, ПРД, моделі загроз, моделі захисту, а також специфікацій гарантій такого захисту дозволяють зробити висновок, що у випадку практичної реалізації названих вище доробок досягнутий рівень гарантованості захисту буде достатнім, щоб сподіватися на беззаперечну довіру клієнтів прикладних інтернет-систем щодо гарантій захисту їхніх персональних даних.

Ключові слова: прикладні інтернет-системи, конфіденційність, персональні дані, транспарентність.

Zander K., Gnatyuk V.

METHODS TO ENHANCE THE GUARANTEED PROTECTION OF PERSONAL DATA IN APPLIED INTERNET SYSTEMS

Existing protection technologies for the operational environment of applied systems do not fully prevent unauthorized actions by administrators with the highest levels of authority, as they do not ensure complete process controllability. This undermines user trust in the guaranteed protection of their personal data.

The most effective way to safeguard the operational environment from external threats is complete isolation. For critical applied applications, this isolation must meet the guarantee criteria of ND TZI 2.5-004-99 at the G-7 level. Ensuring full controllability of this isolation is essential, which is achievable only in internet systems with a transparent software-hardware environment.

It is proposed that the structure of critical applied systems be transparent, and their Functional Protection Profile (FPP) should include an observability service specification according to ND TZI 2.5-004-99. Guaranteeing the correct implementation of this functionality at the G-7 level is a key factor in ensuring client trust. Additionally, the use of theoretically perfect protection methods is substantiated, providing absolute resistance to confidentiality breaches under certain conditions. The corresponding access delimitation rules (ADR) are synthesized, which provide clients with the ability to control the actions of system administrators throughout the entire time the system provides services to its clients. In general, the characteristics of the developed structure, ADR, threat model, protection model, as well as the specifications of the guarantees of such protection allow us to conclude that in the case of practical implementation of the above-mentioned works, the achieved level of guaranteed protection will be sufficient to hope for the unquestionable trust of clients of applied Internet systems regarding the guarantees of protection of their personal data.

Keywords: applied internet systems, confidentiality, personal data, transparency.

Стаття надійшла до редакції 28.02.2025 р.
Прийнято до друку 11.06.2025 р.