НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу

Департамент спеціальних телекомунікаційних систем та
захисту інформації Служби безпеки України

Київ 1999

НОРМАТИВНИЙ ДОКУМЕНТ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України
від “ 28 ” квітня 1999 р. № 22

Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу

НД ТЗІ 1.1-003-99

ДСТСЗІ СБ України
Київ

Передмова

1 РОЗРОБЛЕНО товариством з обмеженою відповідальністю «Інститут комп'ютерних технологій»

2 ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

3 ВВЕДЕНО ВПЕРШЕ

Зміст

НД ТЗІ 1.1-003-99

ТЕРМІНОЛОГІЯ В ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Чинний від 1999-07-01

1 Галузь використання

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Терміни, що установлюються цим документом, обов'язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.

Для кожного поняття встановлено один термін. Застосування синонімів терміна не допускається.

Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів.

2 Нормативні посилання

Під час розробки цього нормативного документа використані наступні стандарти:

- ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення.
- ДСТУ 2941-94. Системи обробки інформації. Розробка систем. Терміни і визначення.
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення.

3 Позначення і скорочення

В цьому НД ТЗІ використовуються наступні позначення і скорочення:

АС — автоматизована система;
КЗЗ — комплекс засобів захисту;
КС — комп'ютерна система;
КСЗІ— комплексна система захисту інформації;
НСД — несанкціонований доступ;
ОС — обчислювальна система;
ПЗ — програмне забезпечення;
ПРД — правила розмежування доступу;
ТЗІ — технічний захист інформації.

4 Терміни і визначення

4.1 Основні поняття

4.1.1 Обчислювальна система; ОС (computer system) — сукупність програмних-апаратних засобів, призначених для обробки інформації.

4.1.2 Автоматизована система; АС (automated system) — організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

4.1.3 Комп'ютерна система; КС (computer system, target of evaluation) —

сукупність програмно-апаратних засобів, яка подана для оцінки.

4.1.4 Політика безпеки інформації (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

4.1.5 Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

4.1.6 Безпека інформації (information security) — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

4.1.7 Захист інформації в АС (information protection, information security, computer system security) — діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

4.1.8 Комплексна система захисту інформації; КСЗІ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

4.1.9 Комплекс засобів захисту; КЗЗ (trusted computing base; TCB) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

4.1.10 Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) — комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

4.1.11 Об'єкт комп'ютерної системи; об'єкт КС (product object, system object) — елемент ресурсу КС, що знаходиться під керуванням КЗЗ і характеризується певними атрибутами і поводженням.

4.1.12 Пасивний об'єкт (passive object) — об'єкт КС, який в конкретному акті доступу виступає як пасивний компонент системи, над яким виконується дія і/або який служить джерелом чи приймальником інформації.

4.1.13 Об'єкт-процес (process object) — виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т.ін.).

4.1.14 Користувач (user) — фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

4.1.15 Об'єкт-користувач (user object) — подання фізичного користувача в КС, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

4.1.16 Ідентифікатор об'єкта КС (object identifier) — унікальний атрибут об'єкта КС, що дозволяє однозначно виділити даний об'єкт серед подібних.

4.1.17 Потік інформації (information flow) — передавання інформації від одного до іншого об'єкта КС.

4.1.18 Доступ до інформації (access to information) — вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до

іншого і/або відбувається зміна стану системи.

4.1.19 Правила розмежування доступу; ПРД (access mediation rules) — частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об’єктів.

4.1.20 Тип доступу (access type) — суттєвість доступу до об’єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

4.1.21 Запит на доступ (access request) — звернення одного об’єкта КС до іншого з метою отримання певного типу доступу.

4.1.22 Санкціонований доступ до інформації (authorized access to information) — доступ до інформації, що не порушує ПРД.

4.1.23 Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) — доступ до інформації, здійснюваний з порушенням ПРД.

4.1.24 Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) — запобігання або істотне утруднення несанкціонованого доступу до інформації.

4.1.25 Право доступу (access right) — дозвіл або заборона здійснення певного типу доступу.

4.1.26 Повноваження (privilege) — права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об’єктів.

4.1.27 Керування доступом (access control) — сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням ПРД.

4.1.28 Розмежування доступу (access mediation) — сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

4.1.29 Авторизація (authorization) — надання повноважень; встановлення відповідності між повідомленням (пасивним об’єктом) і його джерелом (створившим його користувачем або процесом).

4.1.30 Авторизований користувач (authorized user) — користувач, що володіє певними повноваженнями.

4.1.31 Роль користувача (user role) — сукупність функцій щодо керування КС, КЗЗ і обробки інформації, доступних користувачеві.

4.1.32 Адміністратор (administrator, administrative user) — користувач, роль якого включає функції керування КС і/або КЗЗ.

4.1.33 Адміністратор безпеки (security administrator) — адміністратор, відповідальний за дотримання політики безпеки.

4.1.34 Порушник (user violator) — користувач, який здійснює несанкціонований доступ до інформації.

4.2 Властивості інформації і загрози

4.2.1 Ознайомлення (disclosure) — одержання користувачем або процесом інформації, що міститься в об’єкті.

4.2.2 Модифікація (modification) — зміна користувачем або процесом інформації, що міститься в об’єкті.

4.2.3 Критична інформація (sensitive information) — інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

4.2.4 Конфіденційність інформації (information confidentiality) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

4.2.5. Цілісність інформації (information integrity) — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

4.2.6 Цілісність системи (system integrity) — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

4.2.7 Доступність (availability) — властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

4.2.8 Спостереженість (accountability) — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

4.2.9 Атака (attack) — спроба реалізації загрози.

4.2.10 Проникнення (penetration) — успішне подолання механізмів захисту системи.

4.2.11 Вразливість системи (system vulnerability) — нездатність системи протистояти реалізації певної загрози або сукупності загроз.

4.2.12 Компрометація (compromise) — порушення політики безпеки; несанкціоноване ознайомлення.

4.2.13 Втрата інформації (information leakage) — неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

4.2.14 Прихований канал (covert channel) — спосіб одержання інформації за рахунок використання шляхів передачі інформації, існуючих у КС, але не керованих КЗЗ, або спостереження за існуючими потоками інформації.

4.2.15 Прихований канал з пам'яттю (storage covert channel) — прихований канал, що реалізується шляхом прямого або непрямого запису інформації в певну область пам'яті одним процесом і прямим чи непрямим читанням даної області пам'яті іншим процесом.

4.2.16 Часовий прихований канал (timing covert channel) — прихований канал, що дозволяє передавати інформацію від одного процесу до іншого шляхом модулювання першим процесом часових характеристик системи (наприклад, часу зайнятості центрального процесора), що спостерігаються

іншим процесом.

4.2.17 Пропускна здатність прихованого каналу (covert channel bandwidth) — кількість інформації, що одержується використанням прихованого каналу за одиницю часу.

4.2.18 Відмова (fault, failure) — втрата здатності КС або її компонента виконувати певну функцію.

4.2.19 Відмова в обслуговуванні (denial of service) — будь-яка дія або послідовність дій, що призводять будь-яку частину (компонент) системи до виходу із ладу; нездатність системи виконувати свої функції (надавати декларовані послуги) внаслідок виходу із ладу якого-небудь компонента або інших причин.

4.2.20 Невизнання участі (repudiation) — відмова одного з об'єктів КС від факту участі в події, що трапилась.

4.2.21 Відмова від авторства (repudiation of origin) — заперечення причетності до утворення або передачі якого-небудь документа чи повідомлення.

4.2.22 Відмова від одержання (repudiation of receipt) — заперечення причетності до одержання якого-небудь документа або повідомлення.

4.2.23 Комп'ютерний вірус (computer virus) — програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

4.2.24 Програмна закладка (program bug) — потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і/або порушення політики безпеки.

4.2.25 Люк (trap door) — залишені розробником недокументовані функції, використання яких дозволяє обминути механізми захисту.

4.2.26 Троянський кінь (Trojan horse) — програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми.

4.2.27 Збирання сміття — загроза, що полягає в захопленні і аналізі користувачем або процесом спільно використовуваних об'єктів, звільнених іншим користувачем чи процесом, з метою одержання інформації, що в них знаходиться.

4.3 Створення і експлуатація захищених систем

4.3.1 Модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

4.3.2 Модель порушника (user violator model) — абстрактний формалізований або неформалізований опис порушника.

4.3.3 Ризик (risk) — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

4.3.4 Аналіз ризику (risk analysis) — процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС.

4.3.5 Керування ризиком (risk management) — сукупність заходів, що проводяться протягом всього життєвого циклу АС щодо оцінки ризику, вибору, реалізації і впровадження заходів забезпечення безпеки, спрямована на досягнення прийнятного рівня залишкового ризику.

4.3.6 Залишковий ризик (residual risk) — ризик, що залишається після впровадження заходів забезпечення безпеки.

4.3.7 Заходи забезпечення безпеки (safeguards) — послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

4.3.8 Послуга безпеки (security service) — сукупність функцій, що забезпечують захист від певної загрози або від множини загроз.

4.3.9 Механізми захисту (security mechanism) — конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки.

4.3.10 Засоби захисту (protection facility) — програмні, програмно-апаратні та апаратні засоби, що реалізують механізми захисту.

4.3.11 Політика безпеки послуги (service security policy) — правила, згідно з якими функціонують механізми, що реалізують послугу.

4.3.12 Рівень послуги (level of service) — міра ефективності і/або стійкості механізмів, що реалізують послугу, відносно до введеної для даної послуги шкали оцінки.

4.3.13 Гарантії (assurance) — сукупність вимог (шкала оцінки) для визначення міри упевненості, що КС коректно реалізує політику безпеки.

4.3.14 Рівень гарантій (assurance level) — міра упевненості в тому, що КС коректно реалізує політику безпеки.

4.3.15 Модель політики безпеки (security policy model) — абстрактний формалізований або неформалізований опис політики безпеки інформації.

4.3.16 Домен комп'ютерної системи; домен КС (domain) — ізольована логічна область КС, що характеризується унікальним контекстом, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини між собою.

4.3.17 Тестування на проникання (penetration testing) — випробування, метою яких є здійснення спроби обминути або відключити механізми захисту.

4.3.18 Оцінка вразливості (vulnerability assessment) — дослідження об'єкта оцінки з метою визначення можливості реалізації загроз.

4.3.19 Оцінка безпеки інформації (information security evaluation) — процес, метою якого є визначення відповідності стану безпеки інформації в КС встановленим вимогам.

4.3.20 Критерії оцінки захищеності; критерії (security evaluation criteria) — сукупність вимог (шкала оцінки), що використовується для оцінки ефективності функціональних послуг безпеки і коректності їх реалізації.

4.3.21 Рейтинг (rating) — упорядкований перелік рівнів послуг і рівня гарантій, виявлених в процесі оцінки КС.

4.3.22 Функціональний профіль (functionality profile) — упорядкований перелік рівнів функціональних послуг, який може використовуватись як

формальна специфікація функціональності КС.

4.4 Принципи, послуги і механізми забезпечення безпеки

4.4.1 Довірче керування доступом (discretionary access control) — принцип керування доступом, який полягає в тому, що звичайним користувачам дозволено керувати (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домена (наприклад, на підставі права володіння об'єктами) без втручання адміністратора.

4.4.2 Адміністративне керування доступом (mandatory access control) — принцип керування доступом, який полягає в тому, що керувати потоками інформації між користувачами і об'єктами дозволено тільки спеціально авторизованим користувачам, а звичайні користувачі не мають можливості створити потоки інформації, які могли б призвести до порушення встановлених ПРД.

4.4.3 Експорт інформації (information export) — виведення інформації з-під керування КЗЗ назовні.

4.4.4 Імпорт інформації (information import) — уведення інформації ззовні під керування КЗЗ.

4.4.5 Ідентифікація (identification) — процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

4.4.6 Автентифікація (authentication) — процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

4.4.7 Інформація автентифікації (authentication information) — інформація, що використовується для автентифікації.

4.4.8 Пароль (password) — секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.

4.4.9 Персональний ідентифікаційний номер; ПІН (personal identification number, PIN) — вид паролю, що звичайно складається тільки із цифр, і який, як правило, має бути пред'явлений нарівні з носимим ідентифікатором.

4.4.10 Достовірний канал (trusted path) — захищений шлях передачі інформації між користувачем і КЗЗ, що не може бути імітований, а інформація, що передається ним, не може бути отримана або модифікована стороннім користувачем або процесом.

4.4.11 Реєстрація (audit, auditing) — послуга, що забезпечує збирання і аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих КЗЗ.

4.4.12 Журнал реєстрації (audit trail) — упорядкована сукупність реєстраційних записів, кожен з яких заноситься КЗЗ за фактом здійснення контрольованої події.

4.4.13 Довірча конфіденційність (discretionary confidentiality) — послуга, що забезпечує конфіденційність інформації відповідно до принципів довірчого керування доступом.

4.4.14 Адміністративна конфіденційність (mandatory confidentiality) —

послуга, що забезпечує конфіденційність інформації відповідно до принципів адміністративного керування доступом.

4.4.15 Довірча цілісність (discretionary integrity) — послуга, що забезпечує цілісність інформації відповідно до принципів довірчого керування доступом.

4.4.16 Адміністративна цілісність (mandatory integrity) — послуга, що забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

4.4.17 Очищення пам'яті (memory clearing) — знищення даних в пам'яті шляхом встановлення полів цих даних в заданий або випадковий стан.

4.4.18 Розділюваний об'єкт (shared object) — об'єкт КС, який одночасно або почергово використовується різними користувачами і/або процесами.

4.4.19 Повторне використання об'єкта (object reuse) — послуга, що забезпечує очищення пам'яті і призупинення дії повноважень щодо розділюваного об'єкта, який раніше використовувався одним користувачем або процесом, перед наданням його іншому користувачеві або процесу.

4.4.20 Аналіз прихованих каналів (covert channels analyse) — послуга, яка забезпечує гарантію того, що приховані канали в КС відсутні, знаходяться під наглядом або, принаймні, відомі.

4.4.21 Керування потоками (flow control) — сукупність функцій і процедур, які забезпечують неможливість передачі інформації прихованими каналами, тобто в обхід КЗЗ. В більш вузькому значенні часто розуміється сукупність процедур, які забезпечують неможливість передачі інформації від об'єкта КС з більш високим рівнем доступу до об'єкта КС з більш низьким рівнем доступу.

4.4.22 Відкат (rollback) — послуга, що забезпечує повернення об'єкта КС до відомого попереднього стану після виконання над об'єктом певної операції або серії операцій.

4.4.23 Квота (quota) — обмеження можливості використання певного ресурсу КС користувачем або процесом.

4.4.24 Стійкість до відмов (fault tolerance) — послуга, що забезпечує здатність КС продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

4.4.25 Ініціалізація (initialization) — встановлення системи або об'єкта у відомий чи визначений стан.

4.4.26 Диспетчер доступу (reference monitor) — реалізація концепції абстрактного автомата, яка забезпечує дотримання ПРД і характеризується такими трьома особливостями: забезпечує безперервний і повний контроль за доступом, захищений від модифікації і має невеликі розміри.

4.4.27 Ядро захисту (security kernel) — частина КЗЗ, в якій зосереджено мінімально необхідний набір механізмів, що реалізують ПРД.

4.4.28 Атрибут доступу (tag, access mediation information) — будь-яка зв'язана з об'єктом КС інформація, яка використовується для керування доступом.

4.4.29 Матриця доступу (access matrix) — n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об'єктів КС одного типу (об'єктів-користувачів, об'єктів-процесів чи пасивних об'єктів), і містить як елементи

права доступу за кожним із типів доступу.

4.4.30 Список доступу (access control list) — перелік користувачів і/або процесів з зазначенням їх прав доступу до об'єкта КС, з яким пов'язаний цей перелік.

4.4.31 Список повноважень (privilege list, profile) — перелік об'єктів з зазначенням прав доступу до них з боку користувача або процесу, з яким пов'язаний цей перелік.

4.4.32 Мітка (label) — атрибут доступу, що відображає категорію доступу об'єкта КС.

4.4.33 Категорія доступу (security level) — комбінація ієрархічних і неієрархічних атрибутів доступу, що відображає рівень критичності (наприклад, конфіденційності) інформації або повноважень користувача щодо доступу до такої інформації.

4.4.34 Рівень доступу (access level) — ієрархічна частина категорії доступу пасивного об'єкта.

4.4.35 Рівень допуску (clearance) — ієрархічна частина категорії доступу користувача або процесу, що визначає максимальний рівень доступу пасивного об'єкта, до якого може одержати доступ користувач чи процес.

4.4.36 Криптографічне перетворення — перетворення даних, яке полягає в їх шифруванні, вироблення імітовставки або цифрового підпису.

4.4.37 Шифрування даних — процес зашифрування або розшифрування.

4.4.38 Зашифрування даних (data encryption) — процес перетворення відкритого тексту в шифртекст.

4.4.39 Розшифрування даних (data decryption) — процес перетворення шифртексту у відкритий текст.

4.4.40 Відкритий текст (clear text) — дані з доступним семантичним змістом.

4.4.41 Шифртекст (ciphertext) — дані, отримані у результаті зашифрування відкритого тексту.

4.4.42 Ключ (key) — конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

4.4.43 Імітовставка (data authentication code) — блок інформації фіксованої довжини, що одержується із відкритого тексту і ключа, однозначно відповідний даному відкритому тексту.

4.4.44 Цифровий підпис (digital signature) — дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дозволяють приймальнику даних впевнитись в цілісності блоку і справжності джерела даних і забезпечити захист від підробки і підлогу.

4.4.45 Завірення (notarization) — реєстрація даних у довіреної третьої особи з метою забезпечення надалі впевненості в правильності таких характеристик як зміст, джерело даних, час відправлення чи одержання тощо.

5 Список українських термінів в алфавітному порядку

№ п/п	Український термін	Російський термін	Англійський термін	Номер за текстом
1.	автентифікація	аутентификация	authentication	4.4.6
2.	автоматизована система (ас)	автоматизированная система (АС)	automated system	4.1.2
3.	авторизація	авторизация	authorization	4.1.29
4.	авторизований користувач	авторизованный пользователь	authorized user	4.1.30
5.	адміністративна конфіденційність	административная конфиденциальность	mandatory confidentiality	4.4.14
6.	адміністративна цілісність	административная целостность	mandatory integrity	4.4.16
7.	адміністративне керування доступом	административное управлением доступом	mandatory access control	4.4.2
8.	адміністратор	администратор	administrator, administrative user	4.1.32
9.	адміністратор безпеки	администратор безопасности	security administrator	4.1.33
10.	аналіз прихованих каналів	анализ скрытых каналов	covert channels analyse	4.4.20
11.	аналіз ризику	анализ риска	risk analysis	4.3.4
12.	атака	атака	attack	4.2.9
13.	атрибут доступу	атрибут доступа	tag, access mediation information	4.4.28
14.	безпека інформації	безопасность информации	information security	4.1.6
15.	відкат	откат	rollback	4.4.22
16.	відкритий текст	открытый текст	clear text	4.4.40
17.	відмова	отказ	fault, failure	4.2.18
18.	відмова в обслуговуванні	отказ в обслуживании	denial of service	4.2.19
19.	відмова від авторства	отказ от авторства	repudiation of origin	4.2.21
20.	відмова від одержання	отказ от получения	repudiation of receipt	4.2.22
21.	вразливість системи	уязвимость системы	system vulnerability	4.2.11
22.	втрата інформації	утечка информации	information leakage	4.2.13
23.	гарантії	гарантии	assurance	4.3.13
24.	диспетчер доступу	диспетчер доступа	reference monitor	4.4.26
25.	довірча конфіденційність	доверительная конфиденциальность	discretionary confidentiality	4.4.13
26.	довірча цілісність	доверительная целостность	discretionary integrity	4.4.15
27.	довірче управління доступом	доверительное управлением доступом	discretionary access control	4.4.1
28.	домен комп'ютерної системи; домен кс	домен компьютерной системы; домен КС	domain	4.3.16
29.	достовірний канал	достоверный канал	trusted path	4.4.10
30.	доступ до інформації	доступ к информации	access to information	4.1.18
31.	доступність	доступность	availability	4.2.7
32.	експорт інформації	экспорт информации	information export	4.4.3
33.	журнал реєстрації	журнал регистрации	audit trail	4.4.12
34.	завірення	заверение	notarization	4.4.45
35.	загроза	угроза	threat	4.1.5
36.	залишковий ризик	остаточный риск	residual risk	4.3.6
37.	запит доступу	запрос доступа	access request	4.1.21
38.	засоби захисту	средства защиты	protection facility	4.3.10
39.	захист від несанкціонованого доступу; захист від НСД	защита от несанкционированного доступа; защита от НСД	protection from unauthorized access	4.1.24
40.	захист інформації в АС	защита информации в АС	information protection, information security, computer system security	4.1.7

№ п/п	Український термін	Російський термін	Англійський термін	Номер за текстом
41.	захищена комп'ютерна система; захищена КС	защищенная компьютерная система; защищенная КС	trusted computer system, trusted computer product	4.1.10
42.	заходи забезпечення безпеки	меры обеспечения безопасности	safeguards	4.3.7
43.	зашифрування даних	зашифрование данных	data encryption	4.4.38
44.	збирання сміття	сбор мусора		4.2.27
45.	ідентифікатор об'єкта КС	идентификатор объекта КС	object identifier	4.1.16
46.	ідентифікація	идентификация	identification	4.4.5
47.	імітовставка	имитовставка	data authentication code	4.4.43
48.	імпорт інформації	импорт информации	information import	4.4.4
49.	ініціалізація	инициализация	initialization	4.4.25
50.	інформація автентифікації	информация аутентификации	authentication information	4.4.7
51.	категорія доступу	категория доступа	security level	4.4.33
52.	квота	квота	quota	4.4.23
53.	керування доступом	управление доступом	access control	4.1.27
54.	керування потоками	управление потоками	flow control	4.4.21
55.	керування ризиком	управление риском	risk management	4.3.5
56.	ключ	ключ	key	4.4.42
57.	комп'ютерна система (КС)	компьютерная система (КС)	computer system, target of evaluation	4.1.3
58.	комп'ютерний вірус	компьютерный вирус	computer virus	4.2.23
59.	комплекс засобів захисту (КЗЗ)	комплекс средств защиты (КСЗ)	trusted computing base; TCB	4.1.9
60.	комплексна система захисту інформації (КСЗІ)	комплексная система защиты информации (КСЗИ)		4.1.8
61.	компрометація	компрометация	compromise	4.2.12
62.	конфіденційність інформації	конфиденциальность информации	information confidentiality	4.2.4
63.	користувач	пользователь	user	4.1.14
64.	криптографічне перетворення	криптографическое преобразование		4.4.36
65.	критерії оцінки захищеності; критерії	критерии оценки защищенности; критерии	security evaluation criteria	4.3.20
66.	критична інформація	критичная информация	sensitive information	4.2.3
67.	люк	люк	trap door	4.2.25
68.	матриця доступу	матрица доступа	access matrix	4.4.29
69.	механізми захисту	механизмы защиты	security mechanism	4.3.9
70.	мітка	метка	label	4.4.32
71.	модель загроз	модель угроз	model of threats	4.3.1
72.	модель політики безпеки	модель политики безопасности	security policy model	4.3.15
73.	модель порушника	модель нарушителя	user violator model	4.3.2
74.	модифікація	модификация	modification	4.2.2
75.	невизнання участі	непризнание участия	repudiation	4.2.20
76.	несанкціонований доступ до інформації; НСД до інформації	несанкционированный доступ к информации; НСД к информации	unauthorized access to information	4.1.23
77.	об'єкт комп'ютерної системи; об'єкт КС	объект компьютерной системы; объект КС	product object	4.1.11
78.	об'єкт-користувач	объект-пользователь	user object	4.1.15
79.	об'єкт-процес	объект-процесс	process object	4.1.13
80.	Обчислювальна система (ОС)	вычислительная система (ВС)	computer system	4.1.1
81.	ознайомлення	ознакомление	disclosure	4.2.1
82.	оцінка безпеки інформації	оценка безопасности информации	information security evaluation	4.3.19
83.	оцінка вразливості	оценка уязвимости	vulnerability assessment	4.3.18

№ п/п	Український термін	Російський термін	Англійський термін	Номер за текстом
84.	очищення пам’яті	очистка памяти	memory clearing	4.4.17
85.	пароль	пароль	password	4.4.8
86.	пасивний об’єкт	пассивный объект	passive object	4.1.12
87.	персональний ідентифікаційний номер; ПІН	персональный идентификационный номер; ПИН	personal identification number, pin	4.4.9
88.	повноваження	полномочия	privilege	4.1.26
89.	повторне використання об’єкта	повторное использование объекта	object reuse	4.4.19
90.	політика безпеки інформації	политика безопасности информации	information security policy	4.1.4
91.	політика безпеки послуги	политика безопасности услуги	service security policy	4.3.11
92.	порушник	нарушитель	user violator	4.1.34
93.	послуга безпеки	услуга безопасности	security service	4.3.8
94.	потік інформації	поток информации	information flow	4.1.17
95.	правила розмежування доступу (ПРД)	правила разграничения доступа (ПРД)	access mediation rules	4.1.19
96.	право доступу	право доступа	access right	4.1.25
97.	прихований канал	скрытый канал	covert channel	4.2.14
98.	прихований канал з пам’яттю	скрытый канал с памятью	storage covert channel	4.2.15
99.	програмна закладка	программная закладка	program bug	4.2.24
100.	проникнення	проникновение	penetration	4.2.10
101.	пропускна здатність прихованого каналу	пропускная способность скрытого канала	covert channel bandwidth	4.2.17
102.	реєстрація	регистрация	audit, auditing	4.4.11
103.	рейтинг	рейтинг	rating	4.3.21
104.	ризик	риск	risk	4.3.3
105.	рівень гарантій	уровень гарантий	assurance level	4.3.14
106.	рівень допуску	уровень допуска	clearance	4.4.35
107.	рівень доступу	уровень доступа	access level	4.4.34
108.	рівень послуги	уровень услуги	level of service	4.3.12
109.	розмежування доступу	разграничение доступа	access mediation	4.1.28
110.	розділюваний об’єкт	разделяемый объект	shared object	4.4.18
111.	розшифрування даних	расшифрование данных	data decryption	4.4.39
112.	роль користувача	роль пользователя	user role	4.1.31
113.	санкціонований доступ до інформації	санкционированный доступ к информации	authorized access to information	4.1.22
114.	список доступу	список доступа	access control list	4.4.30
115.	список повноважень	список полномочий	privilege list, profile	4.4.31
116.	спостережність	наблюдаемость	accountability	4.2.8
117.	стійкість до відмов	устойчивость к отказам	fault tolerance	4.4.24
118.	тестування на проникнення	тестирование на проникновение	penetration testing	4.3.17
119.	тип доступу	тип доступа	access type	4.1.20
120.	троянський кінь	троянский конь	Trojan horse	4.2.26
121.	функціональний профіль	функциональный профиль	functionality profile	4.3.22
122.	цифровий підпис	цифровая подпись	digital signature	4.4.44
123.	цілісність інформації	целостность информации	information integrity	4.2.5
124.	цілісність системи	целостность системы	system integrity	4.2.6
125.	часовий прихований канал	временной скрытый канал	timing covert channel	4.2.16
126.	шифртекст	шифртекст	ciphertext	4.4.41
127.	шифрування даних	шифрование данных		4.4.37
128.	ядро захисту	ядро защиты	security kernel	4.4.27

6 Список російських термінів в алфавітному порядку

№ п/п	Російський термін	Український термін	Англійський термін	Номер за текстом
1.	автоматизированная система (АС)	автоматизована система (АС)	automated system	4.1.2
2.	авторизация	авторизація	authorization	4.1.29
3.	авторизованный пользователь	авторизований користувач	authorized user	4.1.30
4.	административная конфиденциальность	адміністративна конфіденційність	mandatory confidentiality	4.4.14
5.	административная целостность	адміністративна цілісність	mandatory integrity	4.4.16
6.	административное управлением доступом	адміністративне керування доступом	mandatory access control	4.4.2
7.	администратор	адміністратор	administrator, administrative user	4.1.32
8.	администратор безопасности	адміністратор безпеки	security administrator	4.1.33
9.	анализ риска	аналіз ризику	risk analysis	4.3.4
10.	анализ скрытых каналов	аналіз прихованих каналів	covert channels analyse	4.4.20
11.	атака	атака	attack	4.2.9
12.	атрибут доступа	атрибут доступу	tag, access mediation information	4.4.28
13.	аутентификация	автентифікація	authentication	4.4.6
14.	безопасность информации	безпека інформації	information security	4.1.6
15.	временной скрытый канал	часовий прихований канал	timing covert channel	4.2.16
16.	вычислительная система (ВС)	обчислювальна система (ОС)	computer system	4.1.1
17.	гарантии	гарантії	assurance	4.3.13
18.	диспетчер доступа	диспетчер доступу	reference monitor	4.4.26
19.	доверительная конфиденциальность	довірча конфіденційність	discretionary confidentiality	4.4.13
20.	доверительная целостность	довірча цілісність	discretionary integrity	4.4.15
21.	доверительное управлением доступом	довірче управління доступом	discretionary access control	4.4.1
22.	домен компьютерной системы; домен КС	домен комп'ютерної системи; домен КС	domain	4.3.16
23.	достоверный канал	достовірний канал	trusted path	4.4.10
24.	доступ к информации	доступ до інформації	access to information	4.1.18
25.	доступность	доступність	availability	4.2.7
26.	журнал регистрации	журнал реєстрації	audit trail	4.4.12
27.	заверение	завірення	notarization	4.4.45
28.	запрос доступа	запит доступу	access request	4.1.21
29.	зашифрование данных	зашифрування даних	data encryption	4.4.38
30.	защита информации в АС	захист інформації в АС	information protection, information security, computer system security	4.1.7
31.	защита от несанкционированного доступа; защита от НСД	захист від несанкціонованого доступу; захист від НСД	protection from unauthorized access	4.1.24
32.	защищенная компьютерная система; защищенная КС	захищена комп'ютерна система; захищена КС	trusted computer system, trusted computer product	4.1.10
33.	идентификатор объекта КС	ідентифікатор об'єкта КС	object identifier	4.1.16
34.	идентификация	ідентифікація	identification	4.4.5
35.	имитовставка	імітовставка	data authentication code	4.4.43
36.	импорт информации	імпорт інформації	information import	4.4.4
37.	инициализация	ініціалізація	initialization	4.4.25
38.	информация	інформація автентифікації	authentication information	4.4.7

№ п/п	Російський термін	Український термін	Англійський термін	Номер за текстом
	аутентификации			
39.	категория доступа	категорія доступу	security level	4.4.33
40.	квота	квота	quota	4.4.23
41.	ключ	ключ	key	4.4.42
42.	комплекс средств защиты (КСЗ)	комплекс засобів захисту (КЗЗ)	trusted computing base; TCB	4.1.9
43.	комплексная система защиты информации (КСЗИ)	комплексна система захисту інформації (КСЗІ)		4.1.8
44.	компрометация	компрометація	compromise	4.2.12
45.	компьютерная система (КС)	комп'ютерна система (КС)	computer system, target of evaluation	4.1.3
46.	компьютерный вирус	комп'ютерний вірус	computer virus	4.2.23
47.	конфиденциальность информации	конфіденційність інформації	information confidentiality	4.2.4
48.	криптографическое преобразование	криптографічне перетворення		4.4.36
49.	критерии оценки защищенности; критерии	критерії оцінки захищеності; критерії	security evaluation criteria	4.3.20
50.	критичная информация	критична інформація	sensitive information	4.2.3
51.	люк	люк	trap door	4.2.25
52.	матрица доступа	матриця доступу	access matrix	4.4.29
53.	меры обеспечения безопасности	заходи забезпечення безпеки	safeguards	4.3.7
54.	метка	мітка	label	4.4.32
55.	механизмы защиты	механізми захисту	security mechanism	4.3.9
56.	модель нарушителя	модель порушника	user violator model	4.3.2
57.	модель политики безопасности	модель політики безпеки	security policy model	4.3.15
58.	модель угроз	модель загроз	model of threats	4.3.1
59.	модификация	модифікація	modification	4.2.2
60.	наблюдаемость	спостережність	accountability	4.2.8
61.	нарушитель	порушник	user violator	4.1.34
62.	непризнание участия	невизнання участі	repudiation	4.2.20
63.	несанкционированный доступ к информации; НСД к информации	несанкціонований доступ до інформації; НСД до інформації	unauthorized access to information	4.1.23
64.	объект компьютерной системы; объект КС	об'єкт комп'ютерної системи; об'єкт КС	product object	4.1.11
65.	объект-пользователь	об'єкт-користувач	user object	4.1.15
66.	объект-процесс	об'єкт-процес	process object	4.1.13
67.	ознакомление	ознайомлення	disclosure	4.2.1
68.	остаточный риск	залишковий ризик	residual risk	4.3.6
69.	отказ	відмова	fault, failure	4.2.18
70.	отказ в обслуживании	відмова в обслуговуванні	denial of service	4.2.19
71.	отказ от авторства	відмова від авторства	repudiation of origin	4.2.21
72.	отказ от получения	відмова від одержання	repudiation of receipt	4.2.22
73.	откат	відкат	rollback	4.4.22
74.	открытый текст	відкритий текст	clear text	4.4.40
75.	оценка безопасности информации	оцінка безпеки інформації	information security evaluation	4.3.19
76.	оценка уязвимости	оцінка вразливості	vulnerability assessment	4.3.18
77.	очистка памяти	очищення пам'яті	memory clearing	4.4.17
78.	пароль	пароль	password	4.4.8
79.	пассивный объект	пасивний об'єкт	passive object	4.1.12
80.	персональный идентификационный номер; ПИН	персональний ідентифікаційний номер; ПІН	personal identification number, pin	4.4.9

№ п/п	Російський термін	Український термін	Англійський термін	Номер за текстом
81.	повторное использование объекта	повторне використання об’єкта	object reuse	4.4.19
82.	политика безопасности информации	політика безпеки інформації	information security policy	4.1.4
83.	политика безопасности услуги	політика безпеки послуги	service security policy	4.3.11
84.	полномочия	повноваження	privilege	4.1.26
85.	пользователь	користувач	user	4.1.14
86.	поток информации	потік інформації	information flow	4.1.17
87.	правила разграничения доступа (ПРД)	правила розмежування доступу (ПРД)	access mediation rules	4.1.19
88.	право доступа	право доступу	access right	4.1.25
89.	программная закладка	програмна закладка	program bug	4.2.24
90.	проникновение	проникнення	penetration	4.2.10
91.	пропускная способность скрытого канала	пропускна здатність прихованого каналу	covert channel bandwidth	4.2.17
92.	разграничение доступа	розмежування доступу	access mediation	4.1.28
93.	разделяемый объект	розділюваний об’єкт	shared object	4.4.18
94.	расшифрование данных	розшифрування даних	data decryption	4.4.39
95.	регистрация	реєстрація	audit, auditing	4.4.11
96.	рейтинг	рейтинг	rating	4.3.21
97.	риск	ризик	risk	4.3.3
98.	роль пользователя	роль користувача	user role	4.1.31
99.	санкционированный доступ к информации	санкціонований доступ до інформації	authorized access to information	4.1.22
100.	сбор мусора	збирання сміття		4.2.27
101.	скрытый канал	прихований канал	covert channel	4.2.14
102.	скрытый канал с памятью	прихований канал з пам’яттю	storage covert channel	4.2.15
103.	список доступа	список доступу	access control list	4.4.30
104.	список полномочий	список повноважень	privilege list, profile	4.4.31
105.	средства защиты	засоби захисту	protection facility	4.3.10
106.	тестирование на проникновение	тестування на проникнення	penetration testing	4.3.17
107.	тип доступа	тип доступу	access type	4.1.20
108.	троянский конь	троянський кінь	Trojan horse	4.2.26
109.	угроза	загроза	threat	4.1.5
110.	управление доступом	керування доступом	access control	4.1.27
111.	управление потоками	керування потоками	flow control	4.4.21
112.	управление риском	керування ризиком	risk management	4.3.5
113.	уровень услуги	рівень послуги	level of service	4.3.12
114.	уровень гарантий	рівень гарантій	assurance level	4.3.14
115.	уровень допуска	рівень допуску	clearance	4.4.35
116.	уровень доступа	рівень доступу	access level	4.4.34
117.	услуга безопасности	послуга безпеки	security service	4.3.8
118.	устойчивость к отказам	стійкість до відмов	fault tolerance	4.4.24
119.	утечка информации	втрата інформації	information leakage	4.2.13
120.	уязвимость системы	вразливість системи	system vulnerability	4.2.11
121.	функциональный профиль	функціональний профіль	functionality profile	4.3.22
122.	целостность информации	цілісність інформації	information integrity	4.2.5
123.	целостность системы	цілісність системи	system integrity	4.2.6
124.	цифровая подпись	цифровий підпис	digital signature	4.4.44
125.	шифрование данных	шифрування даних		4.4.37
126.	шифртекст	шифртекст	ciphertext	4.4.41
127.	экспорт информации	експорт інформації	information export	4.4.3
128.	ядро защиты	ядро захисту	security kernel	4.4.27

7 Список англійських термінів в алфавітному порядку

№ п/п	Англійський термін	Український термін	Російський термін	Номер за текстом
1.		комплексна система захисту інформації (КСЗІ)	комплексная система защиты информации (КСЗИ)	4.1.8
2.		криптографічне перетворення	криптографическое преобразование	4.4.36
3.		збирання сміття	сбор мусора	4.2.27
4.		шифрування даних	шифрование данных	4.4.37
5.	access control	керування доступом	управление доступом	4.1.27
6.	access control list	список доступу	список доступа	4.4.30
7.	access level	рівень доступу	уровень доступа	4.4.34
8.	access matrix	матриця доступу	матрица доступа	4.4.29
9.	access mediation	розмежування доступу	разграничение доступа	4.1.28
10.	access mediation rules	правила розмежування доступу (ПРД)	правила разграничения доступа (ПРД)	4.1.19
11.	access request	запит доступу	запрос доступа	4.1.21
12.	access right	право доступу	право доступа	4.1.25
13.	access to information	доступ до інформації	доступ к информации	4.1.18
14.	access type	тип доступу	тип доступа	4.1.20
15.	accountability	спостережність	наблюдаемость	4.2.8
16.	administrator, administrative user	адміністратор	администратор	4.1.32
17.	assurance	гарантії	гарантии	4.3.13
18.	assurance level	рівень гарантій	уровень гарантий	4.3.14
19.	attack	атака	атака	4.2.9
20.	audit trail	журнал реєстрації	журнал регистрации	4.4.12
21.	audit, auditing	реєстрація	регистрация	4.4.11
22.	authentication	автентифікація	аутентификация	4.4.6
23.	authentication information	інформація автентифікації	информация аутентификации	4.4.7
24.	authorization	авторизація	авторизация	4.1.29
25.	authorized access to information	санкціонований доступ до інформації	санкционированный доступ к информации	4.1.22
26.	authorized user	авторизований користувач	авторизованный пользователь	4.1.30
27.	automated system	автоматизована система (АС)	автоматизированная система (АС)	4.1.2
28.	availability	доступність	доступность	4.2.7
29.	ciphertext	шифртекст	шифртекст	4.4.41
30.	clear text	відкритий текст	открытый текст	4.4.40
31.	clearance	рівень допуску	уровень допуска	4.4.35
32.	compromise	компрометація	компрометация	4.2.12
33.	computer system	обчислювальна система (ос)	вычислительная система (ВС)	4.1.1
34.	computer system, target of evaluation	комп'ютерна система (КС)	компьютерная система (КС)	4.1.3
35.	computer virus	комп'ютерний вірус	компьютерный вирус	4.2.23
36.	covert channel	прихований канал	скрытый канал	4.2.14
37.	covert channel bandwidth	пропускна здатність прихованого каналу	пропускная способность скрытого канала	4.2.17
38.	covert channels analyse	аналіз прихованих каналів	анализ скрытых каналов	4.4.20
39.	data authentication code	імітовставка	имитовставка	4.4.43
40.	data decryption	розшифрування даних	расшифрование данных	4.4.39
41.	data encryption	зашифрування даних	зашифрование данных	4.4.38
42.	denial of service	відмова в обслуговуванні	отказ в обслуживании	4.2.19
43.	digital signature	цифровий підпис	цифровая подпись	4.4.44
44.	disclosure	ознайомлення	ознакомление	4.2.1

№ п/п	Англійський термін	Український термін	Російський термін	Номер за текстом
45.	discretionary access control	довірче управління доступом	доверительное управлением доступом	4.4.1
46.	discretionary confidentiality	довірча конфіденційність	доверительная конфиденциальность	4.4.13
47.	discretionary integrity	довірча цілісність	доверительная целостность	4.4.15
48.	domain	домен комп'ютерної системи; домен КС	домен компьютерной системы; домен КС	4.3.16
49.	fault tolerance	стійкість до відмов	устойчивость к отказам	4.4.24
50.	fault, failure	відмова	отказ	4.2.18
51.	flow control	керування потоками	управление потоками	4.4.21
52.	functionality profile	функціональний профіль	функциональный профиль	4.3.22
53.	identification	ідентифікація	идентификация	4.4.5
54.	information confidentiality	конфіденційність інформації	конфиденциальность информации	4.2.4
55.	information export	експорт інформації	экспорт информации	4.4.3
56.	information flow	потік інформації	поток информации	4.1.17
57.	information import	імпорт інформації	импорт информации	4.4.4
58.	information integrity	цілісність інформації	целостность информации	4.2.5
59.	information leakage	втрата інформації	утечка информации	4.2.13
60.	information protection, information security, computer system security	захист інформації в АС	защита информации в АС	4.1.7
61.	information security	безпека інформації	безопасность информации	4.1.6
62.	information security evaluation	оцінка безпеки інформації	оценка безопасности информации	4.3.19
63.	information security policy	політика безпеки інформації	политика безопасности информации	4.1.4
64.	initialization	ініціалізація	инициализация	4.4.25
65.	key	ключ	ключ	4.4.42
66.	label	мітка	метка	4.4.32
67.	level of service	рівень послуги	уровень услуги	4.3.12
68.	mandatory access control	адміністративне керування доступом	административное управлением доступом	4.4.2
69.	mandatory confidentiality	адміністративна конфіденційність	административная конфиденциальность	4.4.14
70.	mandatory integrity	адміністративна цілісність	административная целостность	4.4.16
71.	memory clearing	очищення пам'яті	очистка памяти	4.4.17
72.	model of threats	модель загроз	модель угроз	4.3.1
73.	modification	модифікація	модификация	4.2.2
74.	notarization	завірення	заверение	4.4.45
75.	object identifier	ідентифікатор об'єкта КС	идентификатор объекта КС	4.1.16
76.	object reuse	повторне використання об'єкта	повторное использование объекта	4.4.19
77.	passive object	пасивний об'єкт	пассивный объект	4.1.12
78.	password	пароль	пароль	4.4.8
79.	penetration	проникнення	проникновение	4.2.10
80.	penetration testing	тестування на проникнення	тестирование на проникновение	4.3.17
81.	personal identification number, pin	персональний ідентифікаційний номер; ПІН	персональный идентификационный номер; ПИН	4.4.9
82.	privilege	повноваження	полномочия	4.1.26
83.	privilege list, profile	список повноважень	список полномочий	4.4.31
84.	process object	об'єкт-процес	объект-процесс	4.1.13
85.	product object	об'єкт комп'ютерної системи; об'єкт КС	объект компьютерной системы; объект КС	4.1.11
86.	program bug	програмна закладка	программная закладка	4.2.24

№ п/п	Англійський термін	Український термін	Російський термін	Номер за текстом
87.	protection facility	засоби захисту	средства защиты	4.3.10
88.	protection from unauthorized access	захист від несанкціонованого доступу; захист від НСД	защита от несанкционированного доступа; защита от НСД	4.1.24
89.	quota	квота	квота	4.4.23
90.	rating	рейтинг	рейтинг	4.3.21
91.	reference monitor	диспетчер доступу	диспетчер доступа	4.4.26
92.	repudiation	невизнання участі	непризнание участия	4.2.20
93.	repudiation of origin	відмова від авторства	отказ от авторства	4.2.21
94.	repudiation of receipt	відмова від одержання	отказ от получения	4.2.22
95.	residual risk	залишковий ризик	остаточный риск	4.3.6
96.	risk	ризик	риск	4.3.3
97.	risk analysis	аналіз ризику	анализ риска	4.3.4
98.	risk management	керування ризиком	управление риском	4.3.5
99.	rollback	відкат	откат	4.4.22
100.	safeguards	заходи забезпечення безпеки	меры обеспечения безопасности	4.3.7
101.	security administrator	адміністратор безпеки	администратор безопасности	4.1.33
102.	security evaluation criteria	критерії оцінки захищеності; критерії	критерии оценки защищенности; критерии	4.3.20
103.	security kernel	ядро захисту	ядро защиты	4.4.27
104.	security level	категорія доступу	категория доступа	4.4.33
105.	security mechanism	механізми захисту	механизмы защиты	4.3.9
106.	security policy model	модель політики безпеки	модель политики безопасности	4.3.15
107.	security service	послуга безпеки	услуга безопасности	4.3.8
108.	sensitive information	критична інформація	критичная информация	4.2.3
109.	service security policy	політика безпеки послуги	политика безопасности услуги	4.3.11
110.	shared object	розділюваний об’єкт	разделяемый объект	4.4.18
111.	storage covert channel	прихований канал з пам’яттю	скрытый канал с памятью	4.2.15
112.	system integrity	цілісність системи	целостность системы	4.2.6
113.	system vulnerability	вразливість системи	уязвимость системы	4.2.11
114.	tag, access mediation information	атрибут доступу	атрибут доступа	4.4.28
115.	threat	загроза	угроза	4.1.5
116.	timing covert channel	часовий прихований канал	временной скрытый канал	4.2.16
117.	trap door	люк	люк	4.2.25
118.	Trojan horse	троянський кінь	троянский конь	4.2.26
119.	trusted computer system, trusted computer product	захищена комп’ютерна система; захищена КС	защищенная компьютерная система; защищенная КС	4.1.10
120.	trusted computing base; TCB	комплекс засобів захисту (КЗЗ)	комплекс средств защиты (КСЗ)	4.1.9
121.	trusted path	достовірний канал	достоверный канал	4.4.10
122.	unauthorized access to information	несанкціонований доступ до інформації; НСД до інформації	несанкционированный доступ к информации; НСД к информации	4.1.23
123.	user	користувач	пользователь	4.1.14
124.	user object	об’єкт-користувач	объект-пользователь	4.1.15
125.	user role	роль користувача	роль пользователя	4.1.31
126.	user violator	порушник	нарушитель	4.1.34
127.	user violator model	модель порушника	модель нарушителя	4.3.2
128.	vulnerability assessment	оцінка вразливості	оценка уязвимости	4.3.18