Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно–інформаційних систем і програмної інженерії
(назва факультету)
Комп’ютерних наук
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

Магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Розроблення методики системи захисту комп’ютерної мережі з використанням серверів Stanford University Networks

Виконав: студент (ка) 6 курсу, групи СНм-61
спеціальності (напряму підготовки) 122
Комп’ютерні науки
(шифр і назва спеціальності (напряму підготовки))

		Сеник В.В.
	(підпис)	(прізвище та ініціали)
Керівник		Харченко О.Г.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Мацюк О.В.
	(підпис)	(прізвище та ініціали)
Рецензент		Кареліна О.В.
	(підпис)	(прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Розроблення методики системи захисту комп’ютерної мережі з використанням серверів Stanford University Networks // Дипломна робота ОР «Магістр» // Сеник Валентин Вікторович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНм-61 // - Тернопіль, 2019 // с. – , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: ЗАГРОЗА, ЗАХИСТ, СИСТЕМА, ОБ’ЄКТ, СЕРВЕР, АРХІТЕКТУРА, ДЕСТАБІЛІЗУЮЧИЙ ФАКТОР, МЕТОДИКА, КОНФІДЕНЦІЙНИЙ, НЕСАНКЦІОНОВАНИЙ ДОСТУП.

В першому розділі розглянуто основи систем захисту інформації.

Загрози комп'ютерної безпеки діляться на явні і приховані. Під явними розуміємо такі погрози, які зрозумілі і однозначно передбачені. Вони не вимагають для протидії їм будь-яких додаткових відомостей про статистику погроз і неочевидних припущень про можливі атаки зловмисника.

Критерії оцінки захисту комп'ютера встановлюють базові вимоги щодо контролю комп'ютерної безпеки вбудованої в обчислювальну систему, використовуються, щоб оцінювати, класифікувати та обирати комп'ютерні системи, які використовуються для обробки, зберігання та надання доступу до класифікованої інформації.

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

В другому розділі проаналізовано сервери Sun Microsystems.

Компанія Sun - один з основних виробників серверів, які грають провідну роль в сегменті серверів Інтернету. Ця компанія грає важливу роль в розробці деяких важливих програмних пакетів, використовуваних на веб-сайтах, таких як мова Java і переносні застосування, засновані на Java.

Операційна система Solaris встановлена на всіх комп'ютерах Sun – від настільних комп'ютерів до найбільших корпоративних серверів (еквівалент мейнфрейму компанії Sun). Операційна система Solaris 10 включає ряд інструментальних засобів управління сервером, наведених нижче. Ці інструменти призначені не лише для управління локальною системою, фактично багато хто з них сприяє перетворенню системи Solaris на універсальну консоль управління.

Компанія Sun класифікує сервери відповідно до кількості підтримуваних клієнтів. Інші виробники серверів засновують свої оцінки виходячи з кількості процесорів в сервері. Але в реальному житті все буває набагато складніше. Так, наприклад, сервер класу 1U – це ряд блоків, щільно "упакованих" на стійці, або 16, або 20 коміркових серверів, поміщених в серверній шафі. Тому компанія Sun виробила свій підхід до класифікації серверів, що дозволяє уникнути неоднозначності.

В третьому розділі описано розроблену методику варіанту системи захисту в діючій комп’ютерній мережі.

Об’єкт аналізу – діюча комп’ютерна мережа.

Мета роботи – аналіз роботи діючої мережі підприємства та вдосконалення її захисту; використання при запровадженні оптимізації сервера Sun Microsystems.

Основні результати – проведено аналіз об’єктів загроз, аналіз критеріїв оцінки інформаційної безпеки, аналіз існуючих категорій серверів; розроблено методику вибору варіанту системи захисту за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів, розроблено методику використання систем захисту конфіденційної інформації.

ANNOTATION

Development of technique of computer network security system using Stanford University Networks servers // Diploma thesis Master degree // Senyk Valentyn // Ternopil Ivan Pul'uj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Computer Science , a group SNm-61 // Ternopil, 2019 // Page - , Fig. - , Table - , Draws - .

Lately a report is about attacks on information, about hackers and computer взломи filled all mass medias. That such the "attack on information"? To give determination to this action in actual fact very difficultly, as information, especially in an electronic kind, presented by hundreds of different kinds. It is possible to consider a separate file, and database, and one record information in her, and complete programmatic complex. And all these objects can yield and yield to the attacks from the side of some task force of persons.

At storage, support and grant to access to any information holding object his proprietor, or a person is authorized to them, lays on obviously or self-evident set of rules on work with her. Intentionally their violation is classified as an attack on information.

With mass introduction of computers in all spheres of activity of man there is a volume of information which is kept in an electronic kind grew in thousand one times. And now to copy for a half-minute and bear a diskette with a file which contains the plan of producing of products, far simpler than copy or to rewrite the stack of papers. And with appearance of computer networks even absence of physical access to the computer left off to be the guarantee of maintenance of information.

Are there what possible consequences of attacks on information? First of all, certainly, us economic losses will interest:

1. Opening of commercial information can result in serious proximate damages at the market.

2. Information about the theft of high-cube of information usually in earnest influences on reputation of firm, resulting side in losses in the volumes of trade operations.

3. Firms-competitors can take advantage of theft of information, if and remained unnoticed, in an order fully to bring to ruin a firm, imposing dummy or consciously unprofitable activities to her.

4. Substitution of information both on the stage of transmission and on the stage of storage in a firm can result in enormous losses.

5. Frequent successful attacks on a firm which gives any type of informative services reduce a trust to the firm for clients, that affects volume of profits.

Naturally, computer attacks can bring an enormous moral loss. In itself clearly, that no user of computer network does not want, that his folias except for an addressee got 5-10 persons yet, or, for example, your text which takes computer on a keyboard was copied in a buffer, and then during connecting to the Internet left on a certain server. Namely place is so taken in thousands and ten of thousands of cases.

A few interesting numbers are about attacks on information. They were got the research center of DataPro Research in 1998 year. Principal reasons of damages of electronic information were distributed thus: unintentional error of man - 52% cases, intentional actions of man - 10% cases, refuse of technique - 10% cases, damage as a result of fire - 15% cases, damage - 10% cases water. As evidently, every tenth case of damage of electronic data is related to the computer attacks.

Who was the performer of these actions: at 81% cases is current skilled composition of establishments, only at 13% cases are absolutely extraneous people, and at 6% cases - former workers of the same establishments. Part of attacks, producible employees firms and enterprises, simply stuns and compels to reminisce not only technical but also about psychological methods the prophylaxises of similar actions.

And, finally, that malefactors do exactly, getting to information: at the 44% cases of hacking the direct thefts of money were conducted from electronic accounts,

at 16% cases software hatched from a line-up, so often - at 16% cases - the theft of information was conducted with different consequences, at 12% cases information was falsified, at 10% cases malefactors by means of computer availed or ordered services to which in principle must not were have an access.

Actuality of work is application of the systems of defence of confidential information in the operating computer systems.

A research purpose is: to analyse work of operating network of enterprise and perfect her defence; to use the server of Sun Microsystems for the input of optimization.

The basic tasks of work are: analysis of requirements to defence of computer information; analysis of objects of threats; analysis of criteria of estimation of informative safety; analysis of existent categories of servers; development of methods of choice of variant of the system of defence on the criterion of vitality in the conditions of vagueness of influence of destabilizing factors, practical application of the systems of defence of confidential information.

An object of analysis is an operating computer network.

Basic results - the analysis of objects of threats, analysis of criteria of estimation of informative safety, analysis of existent categories of servers, is conducted; the methods of choice of variant of the system of defence on the criterion of vitality in the conditions of vagueness of influence of destabilizing factors, developed methods of the use of the systems of defence of confidential information are worked out.

The novelty of results is conduct research there is application of the worked out methods of choice of variant of the system of defence on the criterion of vitality in the conditions of vagueness of influence of destabilizing factors.

Keywords: THREAT, DEFENCE, SYSTEM, OBJECT, SERVER, ARCHITECTURE, DESTABILIZING FACTOR, METHODS, CONFIDENTIAL, UNAUTHORIZED DIVISION.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AH – Authentication Header

CIA – Confidentiality, Integrity and Availability

CISC – complex instruction set computer (процесор із складним набором команд)

DR – Dynamic Reconfiguration (динамічна реконфігурація)

ECITS – Evaluation Criteria for IT Security (Критерії оцінки безпеки інформаційних технологій)

ESP – Encapsulating Security Payload

IKE – Internet Key Exchange

MBR – Master Boot Record (головний завантажувальний запис)

NSB – Non-System Bootstrap (несистемний завантажувач)

POST – Power-On Self-Test (самотестування комп’ютера)

RISC – reduced instruction set computer (процесор із скороченим набором команд)

SKIP – Simple Key management for Internet Protocol (просте керування ключами для IP-протоколу)

TCSEC – Trusted Computer System Evaluation Criteria (Критерії оцінки захисту комп'ютера)

АС – автоматизовані системи

ДФ – дестабілізуючі фактори

ЕЦП – електронний цифровий підпис

ЗЗІ – засоби захисту інформації

ЗОТ – засоби обчислювальної техніки

КМЗ – корпоративні мережі зв'язку

ЛПР – людина, яка приймає рішення

НЖМД – накопичувач на жорсткому магнітному диску

НСД – несанкціонований доступ

ПЗ – програмне забезпечення

РПД – розмежувальна політика доступу

СЗІ – системи захисту інформації

СЗКІ – система захисту конфіденційної інформації

ЦС – Центр сертифікації

ЗМІСТ

ВСТУП

Останнім часом повідомлення про атаки на інформацію, про хакерів і комп'ютерні взломи наповнили всі засоби масової інформації. Що ж таке "атака на інформацію"? Дати визначення цій дії насправді дуже складно, оскільки інформація, особливо в електронному вигляді, представлена сотнями різних видів. Інформацією можна вважати і окремий файл, і базу даних, і один запис в ній, і повний програмний комплекс. І всі ці об'єкти можуть піддатися і піддаються атакам з боку деякої соціальної групи осіб.

При зберіганні, підтримці і наданні доступу до будь-якого інформаційного об'єкту його власник, або уповноважена ним особа, накладає явно або самоочевидно набір правил по роботі із нею. Навмисне їх порушення класифікується як атака на інформацію.

Із масовим впровадженням комп'ютерів у всі сфери діяльності людини об'єм інформації, що зберігається в електронному вигляді виріс в тисячі разів. І тепер скопіювати за півхвилини і понести дискету із файлом, що містить план випуску продукції, набагато простіше, ніж зкопіювати або переписати кіпу паперів. А із появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією збереження інформації.

Які можливі наслідки атак на інформацію? В першу чергу, звичайно, нас цікавитимуть економічні втрати:

1. Розкриття комерційної інформації може привести до серйозних прямих збитків на ринку

2. Звістка про крадіжку великого об'єму інформації зазвичай серйозно впливає на репутацію фірми, приводячи побічно до втрат в об'ємах торгових операцій

3. Фірми-конкуренти можуть скористатися крадіжкою інформації, якщо та залишилася непоміченою, для того, щоб повністю розорити фірму, нав'язуючи їй фіктивні або свідомо збиткові операції

4. Підміна інформації як на етапі передачі, так і на етапі зберігання у фірмі може привести до величезних збитків

5. Багатократні успішні атаки на фірму, що надає будь-який вид інформаційних послуг, знижують довіру до фірми у клієнтів, що позначається на об'ємі доходів.

Природно, комп'ютерні атаки можуть принести і величезний моральний збиток. Поняття конфіденційного спілкування давно вже стало "притчею во язицех". Само собою зрозуміло, що ніякому користувачеві комп'ютерної мережі не хочеться, щоб його листи окрім адресата отримували ще 5-10 чоловік, або, наприклад, ваш текст, що набирається на клавіатурі ЕОМ, копіювався в буфер, а потім при підключенні до Інтернету відправлявся на певний сервер. А саме так і відбувається в тисячах і десятках тисяч випадків.

Декілька цікавих цифр про атаки на інформацію. Вони були отримані дослідницьким центром DataPro Research в 1998 році. Основні причини пошкоджень електронної інформації розподілилися таким чином: ненавмисна помилка людини – 52% випадків, умисні дії людини - 10% випадків, відмова техніки – 10% випадків, пошкодження в результаті пожежі - 15% випадків, пошкодження водою – 10% випадків. Як видно, кожен десятий випадок пошкодження електронних даних пов'язаний з комп'ютерними атаками.

Хто був виконавцем цих дій: у 81% випадків – поточний кадровий склад установ, тільки в 13% випадків – абсолютно сторонні люди, і в 6% випадків – колишніх працівників цих же установ. Частка атак, вироблюваних співробітниками фірм і підприємств, просто приголомшує і примушує пригадати не тільки про технічні, але і про психологічні методи профілактики подібних дій.

І, нарешті, що ж саме роблять зловмисники, дістався до інформації: у 44% випадків взлому були проведені безпосередні крадіжки грошей з електронних рахунків, в 16% випадків виводилося з ладу програмне забезпечення, так же часто – в 16% випадків – проводилася крадіжка інформації з різними наслідками, в 12% випадків інформація була сфальсифікована, в 10%

випадків зловмисники за допомогою комп'ютера скористалися або замовили послуги, до яких в принципі не повинні були мати доступу.

Актуальністю роботи є застосування систем захисту конфіденнційної інформації в діючих комп’ютерних системах.

Метою дослідження є: проаналізувати роботу діючої мережі підприємства та вдосконалити її захист; використати при запровадженні оптимізації сервер Sun Microsystems.

Основними завданнями роботи є: аналіз вимог до захисту комп’ютерної інформації; аналіз об’єктів загроз; аналіз критеріїв оцінки інформаційної безпеки; аналіз існуючих категорій серверів; розробка методики вибору варіанту системи захисту за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів, практичне застосування систем захисту кофіденційної інформації.

Новизною результатів проведено дослідження є застосування розробленої методики вибору варіанту системи захисту за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів.

1 ОСНОВИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Вимоги до захисту комп’ютерної інформації

Природним ходом розвитку інформаційних технологій став принциповий перехід від відкритості до захищеності при побудові інформаційних систем. На сьогодні більшість програмних продуктів, що застосовуються для побудови інформаційних систем, мають вбудовані засоби захисту. Це стосується не лише ОС, але СУБД і інших застосувань. Наприклад, замість протоколу IPv4.0, спочатку створеного для реалізації єдиного відкритого мережевого простору, пропонується протокол, що містить розвинені можливості забезпечення інформаційної безпеки. Таким чином, спостерігається загальна тенденція посилення ролі механізмів захисту в сучасних інформаційних і мережевих технологіях.

Цю тенденцію наочно ілюструє розвиток ОС MS Windows. Можна чітко прослідкувати розвиток вбудованих в ОС механізмів захисту від Windows 3.1 (де механізми захисту практично були відсутні), до Windows NT (де механізми захисту інтегровані в ядро ОС) і до Windows 2000 (де інтеграція захоплює і зовнішні по відношенню до розробників технології захисту, такі як Kerberos, і так далі). Те ж саме можна сказати і про інші сімейства ОС. Наприклад, в ОС FreeBSD в кожній з нових версій з'являються нові механізми захисту (firewall, nat). Такий же розвиток засобів захисту стосується і прикладного програмного забезпечення (ПЗ). В СУБД (Oracle) розвиток захисних механізмів виражається в шифруванні трафіку, ускладненні авторизації, додаванні розмежування доступу до елементів таблиць і тому подібне.

З урахуванням сказаного виникає низка запитань :

1. Чи достатньо вбудованих в сучасних ОС і застосування механізмів

захисту для забезпечення гарантованого захисту інформації від НСД?

2. У припущенні, що вбудованих механізмів захисту недостатньо (а з урахуванням існуючої статистики погроз це саме так), то чим це викликано? Чому захищеність комп'ютерної інформації залишається недостатньою, незважаючи на стійку тенденцію до підсилення вбудованих в сучасних універсальних ОС і застосування механізмів захисту? Яким чином слід підсилювати вбудовані механізми додатковими засобами захисту?

3. Які функції повинні забезпечувати і які характеристики повинні мати системи вбудованого і додаткового захисту, щоб забезпечити надійну протидію спробам НСД?

4. У припущенні, що додаткові механізми захисту необхідні, яким чином комплексувати (взаємозв'язвувати) в захищуваній обчислювальній системі вбудовані і додаткові механізми захисту?

Використовувані нині на практиці підходи до захисту комп'ютерної інформації визначаються наступним характеристиками:

– формалізованими вимогами до набору і параметрів механізмів захисту, що регламентують сучасні вимоги до забезпечення комп'ютерної безпеки (вимогами, що визначають що має бути);

– реальними механізмами захисту, що реалізовуються при захисті комп'ютерної інформації. До таких відносяться раніше всього засоби захисту ОС, оскільки більшість застосувань використовують вбудовані в ОС механізми захисту (що визначають, що є);

– існуючою статистикою погроз комп'ютерної безпеки – ісмнуючими успішними атаками на інформаційні комп'ютерні ресурси (що визначають, наскільки ефективне те, що є і даючими оцінку достатності вимог до того, що повинно бути).

Класифікація вимог до систем захисту.

У загальному випадку слід говорити про необхідність врахування двох (які доповнюють один одного) груп вимог до системи захисту.

Перша група вимог (необхідні вимоги) полягає в необхідності реалізації системою захисту формалізованих заходів безпеки (тобто заходів, заданих відповідними нормативними документами в області захисту інформації).

Формалізовані вимоги до необхідних механізмів захисту інформаційних систем, в частині їх захисту від НСД, сформульовані у відповідних керівних документах.

При цьому відмітимо, що ці документи носять загальний характер. В них не повною мірою передбачається класифікація об'єктів, для яких має бути реалізований захист. Та напевно, це і неможливо у рамках одного документу. Зокрема, ці документи пред'являють єдині вимоги для всіх сімейств ОС. І це не дивлячись на те, що ОС різних сімейств мають принципово відмінні принципи побудови, а значить, для них відрізняються і способи НСД.

У вказаних керівних документах не дається рекомендацій по способам побудови і адміністрування захищених систем, тобто не сказано, як їх будувати. У цих документах лише сформульовані вимоги (що має бути реалізовано) до механізмів захисту інформації і, частково, вимоги до їх кількісних характеристик.

Цей підхід до завдання формалізованих вимог, напевно, в цілому виправданий, оскільки неможливо врахувати в нормативних документах всі тонкощі побудови і проектування засобів захисту складних інформаційних систем, особливо при існуючій динаміці їх розвитку.

Друга група вимог (додаткові вимоги) полягає в необхідності обліку існуючої (поточної) статистики погроз для конкретного типу об'єкту, що захищається, а також потенційно можливих погроз. Необхідність цієї групи вимог обумовлена тим, що формалізовані вимоги не можуть враховувати усі можливі погрози об'єктам усіх типів, що вимагають захисту. Також формалізовані вимоги не можуть змагатися за швидкістю оновлення із швидкістю зміни статистики погроз.

1.1.1 Формалізовані вимоги до захисту і їх класифікація

Як було наведено вище, загальні підходи в системах захисту варто розглядати відносно відповідності їх прийнятим формалізованим вимогам. Ці вимоги пред'являються до механізмів захисту, які в тій чи іншій мірі реалізуються сучасними ОС, застосуваннями і додатковими засобами захисту.

Захист інформації від НСД регламентують нормативні документи [1, 2]:

– Вимоги до захисту засобів обчислювальної техніки (ЗОТ) [1], формалізують умови захищеності окремо взятого засобу - ОС, СУБД, застосування.

– Вимоги до захисту автоматизованих систем (АС) [2], формалізують умови захищеності об'єкту з обліком:

– сукупності механізмів захисту, що реалізовуються встановленими на захищуваному об'єкті засобами, включаючи ОС, СУБД (якщо є), застосуваннями, додатковими механізмами захисту (якщо є);

– додаткових організаційних заходів, що приймаються для безпечного функціонування АС.

При цьому відмітимо, що, як правило, застосування використовують механізми захисту ОС. Що стосується СУБД, то механізми захисту СУБД доповнюють захисні механізми ОС, оскільки виникає необхідність захисту додаткових об'єктів доступу - "таблиць". І дійсно, для ОС захищуваними файловими об'єктами є: логічні диски (томи), каталоги, файли. При роботі з базами даних складність обумовлена тим, що таблиці різних користувачів, до яких повинен розмежовуватися доступ, можуть знаходитися в одному файлі. Таким чином, виходить, що в загальному випадку неможливо керувати доступом до баз даних тільки механізмами захисту ОС. Проте це відноситься тільки до СУБД. Інші застосування зазвичай задовільняються захисними механізмами ОС. Тобто, можна сказати, що, як правило, усі механізми захисту автоматизованих систем (АС) по замовчуванню реалізуються власне ОС.

В загальному випадку формалізовані вимоги до забезпечення захисту комп'ютерної інформації від НСД (тобто до засобів захисту ОС) задаються формалізованими вимогами до захисту засобів обчислювальної техніки (ЗОТ)

[1]. Згідно вищенаведеного, будемо для оцінки ефективності захисних механізмів ОС також використовувати формалізовані вимоги з документу [2], застосовувані до автоматизованих систем (АС). Це слід робити, тому що саме захисні механізми ОС покликані забезпечувати необхідний рівень захисту автоматизованої системи (АС) в цілому.

Аналогічні міркування можуть бути проведені і відносно засобу додаткового захисту. При цьому, по-перше, він може розглядатися як окремий ЗОТ, що виконує формалізовані вимоги документу [1]. В цьому випадку вбудовані в ОС механізми захисту не повинні розглядатися. А по-друге, він може розглядатися як засіб в складі АС (разом з механізмами ОС, доповнюючи їх). В цьому випадку вбудовані в ОС і додаткові механізми захисту повинні в сукупності виконувати формалізовані вимоги документу [2]. Крім того, для певних класів захисту вбудовані механізми захисту мають бути сертифіковані.

Розглянемо формалізовані вимоги до захисту комп'ютерної інформації АС відповідно до документу [2]. При цьому будемо розглядати першу групу АС (відповідно до використовуваної в [2] класифікації), що включає найбільш поширені розраховані на багато користувачів АС, в яких одночасно обробляється і/або зберігається інформація різних рівнів конфіденційності. Причому не всі користувачі мають право доступу до всієї інформації АС.

Перша група АС містить п'ять класів - 1Д, 1Г, 1В, 1Б і 1А. Поділ АС на відповідні класи за умовами їх функціонування з точки зору захисту інформації необхідний в цілях розробки і застосування обгрунтованих заходів по досягненню необхідного рівня захисту. Диференціація підходу до вибору методів і засобів захисту визначається важливістю оброблюваної інформації, а також відмінністю АС по своєму складу, структурі, способам обробки інформації, кількісному і якісному складу користувачів і обслуговуючого персоналу [2].

Вимоги до АС першої групи приведені в таблиці 1.1.

Таблиця 1.1 – Формалізовані вимоги до захисту інформації від НСД

Підсистеми і вимоги	Класи				
	1Д	1Г	1В	1Б	1А
1. Підсистема управління доступом					
1.1 Ідентифікація, перевірка достовірності і контроль доступу суб'єктів:					
– в систему	+	+	+	+	+
– до терміналів, ЕОМ, вузлів мережі ЕОМ, каналів зв'язку, зовнішнім пристроям ЕОМ	–	+	+	+	+
– до програм	–	+	+	+	+
– до томів, каталогів, файлів, записів, полів записів	–	+	+	+	+
1.2. Управління потоками інформації	–	–	+	+	+
2. Підсистема реєстрації і обліку					
2.1. Реєстрація і облік:					
– входу (виходу) суб'єктів доступу в (із) систему (вузол мережі)	+	+	+	+	+
– видачі друкованих (графічних) вихідних документів	–	+	+	+	+
– запуску (завершення) програм і процесів (задач, завдань)	–	+	+	+	+
– доступу програм суб’єктів доступу до файлів, що захищаються, включаючи їх створення, видалення, передачу по лініях і каналах зв'язку	–	+	+	+	+
– доступу програм суб'єктів доступу до терміналів, ЕОМ, вузлам мережі ЕОМ, програмам, томам, каталогам, файлам, записам, полям записів	–	+	+	+	+
– зміни повноважень суб'єктів доступу	–	–	+	+	+
– створюваних об'єктів доступу, що захищаються	–	–	+	+	+
2.2. Облік носіїв інформації	+	+	+	+	+
2.3. Очищення (обнулення, знеособлення) звільнюваних областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів	–	+	+	+	+
2.4. Сигналізація спроб порушення захисту	–	–	+	+	+
3. Криптографічна підсистема					
3.1. Шифрування конфіденційної інформації	–	–	–	+	+
3.2. Шифрування інформації, яка належить різним суб'єктам доступу (групам суб'єктів) на різних ключах	–	–	–	–	+
3.3. Використання атестованих (сертифікованих) криптографічних засобів	–	–	–	+	+

Продовження таблиці 1.1

Підсистеми і вимоги	Класи				
	1Д	1Г	1В	1Б	1А
4. Підсистема забезпечення цілісності					
4.1. Забезпечення цілісності програмних засобів і оброблюваної інформації	+	+	+	+	+
4.2. Фізична охорона засобів обчислювальної техніки і носіїв інформації	+	+	+	+	+
4.3. Наявність адміністратора (служби) захисту інформації в АС	–	–	+	+	+
4.4. Періодичне тестування СЗІ НСД	+	+	+	+	+
4.5. Наявність засобів відновлення СЗІ НСД	+	+	+	+	+
4.6. Використання сертифікованих засобів захисту	–	–	+	+	+

“–” немає вимог до цього класу;

“+” є вимоги до цього класу.

Як бачимо, даними вимогами виділяються наступні основні групи механізмів захисту:

– механізми керування доступом;

– механізми реєстрації і обліку;

– механізми криптографічного захисту;

– механізми контролю цілісності.

Відмітимо, що перша група “Підсистема управління доступом” є засадою для реалізації захисту від НСД, оскільки саме механізми захисту цієї групи покликані безпосередньо протидіяти несанкціонованому доступу до комп'ютерної інформації.

Інші ж групи механізмів реалізуються в припущенні, що механізми захисту першої групи можуть бути здолані зловмисниками. Зокрема вони можуть використовуватися:

– для контролю дій користувача - група “Підсистема реєстрації і обліку”;

– для протидії можливості прочитання викраденої інформації (наприклад, значень паролів і даних) - група “Криптографічна підсистема”;

– для контролю здійснених зловмисником змін захищуваних об'єктів (виконуваних файлів і файлів даних) при здійсненні до них НСД і для відновлення захищуваної інформації з резервних копій – група “Підсистема забезпечення цілісності”.

Крім того, ці групи механізмів можуть використовуватися для проведення розслідування за фактом НСД.

Розглянемо детальніше вимоги різних груп (згідно [2]), а також відповідні їм основні підходи до захисту комп'ютерної інформації, що реалізовуються на сьогодні на практиці. При цьому має сенс зупинитися лише на двох класах :

– 1Г, задаючим необхідні (мінімальні) вимоги для обробки конфіденційної інформації;

– 1В, задаючим необхідні (мінімальні) вимоги для обробки інформації, власністю держави і віднесеної до категорії секретної.

1.1.2 Вимоги до захисту конфіденційної інформації

Підсистема управління доступом повинна задовольняти наступним вимогам:

1. Ідентифікувати і перевіряти достовірність суб'єктів доступу при вході в систему. Причому це повинно здійснюватися по ідентифікатору (коду) і паролю умовно-постійної дії завдовжки не менше шести буквено-цифрових символів.

2. Ідентифікувати термінали, ЕОМ, вузли комп'ютерної мережі, канали зв'язку, зовнішні пристрої ЕОМ по їх логічних адресах (номерам).

3. По іменах ідентифікувати програми, томи, каталоги, файли, записи і поля записів.

4. Здійснювати контроль доступу суб'єктів до ресурсів, що захищаються, відповідно до матриці доступу.

Підсистема реєстрації і обліку повинна:

1. Реєструвати вхід (вихід) суб'єктів доступу в систему (із системи), або реєструвати завантаження і ініціалізацію операційної системи і її програмної зупинки. При цьому в параметрах реєстрації вказуються:

– дата і час входу (виходу) суб'єкта доступу в систему (із системи) або завантаження (зупинки) системи;

– результат спроби входу – успішни або неуспішний (при НСД);

– ідентифікатор (код або прізвище) суб'єкта, пред'явлений при спробі доступу;

– код або пароль, пред'явлений при спробі неуспіху.

Реєстрація виходу з системи або зупинка не проводиться в моменти апаратурного відключення АС.

2. Реєструвати видачу друкованих (графічних) документів на “тверду” копію. При цьому в параметрах реєстрації вказуються:

– дата і час видачі (звернення до підсистеми виводу);

– короткий зміст документу (найменування, вид, код, шифр) і рівень його конфіденційності;

– специфікація пристрою видачі (логічне ім'я (номер) зовнішнього пристрою);

– ідентифікатор суб'єкта доступу, що запросив документ.

3. Реєструвати запуск (завершення) програм і процесів (задач, завдань), призначених для обробки файлів, що захищаються. При цьому в параметрах реєстрації вказується:

– дата і час запуску;

– ім'я (ідентифікатор) програми (процесу, завдання);

– ідентифікатор суб'єкта доступу, що запросив програму (процес, завдання);

– результат запуску (успішний, неуспішний – несанкціонований).

– Реєструвати спроби доступу програмних засобів (програм, процесів, задач, завдань) до захищуваних файлів. В параметрах реєстрації вказується:

– дата і час спроби доступу до захищуваного файлу з вказуванням її результату (успішний, неуспішний – несанкціонований);

– ідентифікатор суб'єкта доступу;

– специфікація захищуваного файлу.

4. Реєструвати спроби доступу програмних засобів до наступних додаткових захищуваних об'єктів доступу: терміналам, ЕОМ, вузлам мережі ЕОМ, лініям (каналам) зв'язку, зовнішнім пристроям ЕОМ, програмам, томам, каталогам, файлам, записам, полям записів. При цьому в параметрах реєстрації вказується:

– дата і час спроби доступу до захищуваного файлу із вказуванням її результату: успішний, неуспішний, несанкціонований;

– ідентифікатор суб'єкта доступу;

– специфікація захищуваного об'єкту [логічне ім'я (номер)].

5. Проводити облік усіх захищуваних носіїв інформації за допомогою їх маркування та із занесенням облікових даних в журнал (облікову картку).

6. Реєструвати видачу (приймання) захищуваних носіїв.

7. Здійснювати очищення (обнулення, знеособлення) вивільнюваних областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів. При цьому очищення повинно проводитися одноразовим довільним записом в область вивільнюваної пам'яті, раніше використану для зберігання захищуваних даних (файлів).

Підсистема забезпечення цілісності повинна:

1. Забезпечувати цілісність програмних засобів системи захисту інформації від НСД (СЗІ НСД), оброблюваної інформації, а також незмінність програмного середовища. При цьому:

– цілісність СЗІ НСД перевіряється при завантаженні системи по контрольних сумах компонент СЗІ;

– цілісність програмного середовища забезпечується використанням трансляторів з мови високого рівня і відсутністю засобів модифікації об'єктного коду програм в процесі обробки і (або) зберігання захищуваної інформації.

2. Здійснювати фізичну охорону ЗОТ (пристроїв і носіїв інформації). При цьому повинні передбачатися контроль доступу в приміщення АС сторонніх осіб, а також наявність надійних завад для несанкціонованого проникнення в приміщення АС і сховище носіїв інформації. Особливо в неробочий час.

3. Проводити періодичне тестування функцій СЗІ НСД при зміні програмного середовища і персоналу АС за допомогою тест-програм, що імітують спроби НСД.

4. Мати в наявності засоби відновлення СЗІ НСД. При цьому передбачається ведення двох копій програмних засобів СЗІ НСД, а також їх періодичне оновлення і контроль працездатності.

1.1.3 Вимоги до захисту секретної інформації

Підсистема управління доступом повинна:

1. Ідентифікувати і перевіряти достовірність суб'єктів доступу при вході в систему. Причому це повинно здійснюватися по ідентифікатору (коду) і паролю умовно-постійної дії завдовжки не менше шести буквено-цифрових символів.

2. Ідентифікувати термінали, ЕОМ, вузли комп'ютерної мережі, канали зв'язку, зовнішні пристрої ЕОМ по їх логічних адресах (номерах).

3. По іменах ідентифікувати програми, томи, каталоги, файли, записи і поля записів.

4. Здійснювати контроль доступу суб'єктів до захищуваних ресурсів відповідно до матриці доступу.

5. Керувати потоками інформації за допомогою міток конфіденційності. При цьому рівень конфіденційності накопичувача повинен бути не нижче рівня конфіденційності записуваної на нього інформації.

Підсистема реєстрації і обліку повинна:

1. Реєструвати вхід (вихід) суб'єктів доступу в систему (з системи) або реєструвати завантаження і ініціалізацію операційної системи і її програмної зупинки. При цьому в параметрах регістрації вказуються:

– дата і час входу (виходу) суб'єкта доступу в систему (з системи) або завантаження (зупинки) системи;

– результат спроби входу – успішний або неуспішний (при НСД);

– ідентифікатор (код або прізвище) суб'єкта, пред'явлений при спробі доступу;

– код або пароль, пред'явлений при спробі неуспіху.

Реєстрація виходу з системи або зупинку не проводиться в моменти апаратурного відключення АС.

2. Реєструвати видачу друкованих (графічних) документів на “тверду” копію. Видача повинна супроводжуватися автоматичним маркуванням кожного листа (сторінки) документу порядковим номером і обліковими реквізитами АС з вказуванням на останньому листі документу загальної кількості сторінок. В параметрах реєстрації вказуються:

– дата і час видачі (звернення до підсистеми виводу);

– короткий зміст документу (найменування, вид, код, шифр) і рівень його конфіденційності;

– специфікація пристрою видачі (логічне ім'я (номер) зовнішнього пристрою);

– ідентифікатор суб'єкта доступу, що запросив документ;

– об'єм фактично виданого документу (кількість сторінок, листів, копій) і результат видачі (успішний – весь об'єм, неуспішний).

3. Реєструвати запуск (завершення) програм і процесів (задач, завдань), призначених для обробки захищуваних файлів. В параметрах реєстрації вказується:

– дата і час запуску;

– ім'я (ідентифікатор) програми (процесу, завдання);

– ідентифікатор суб'єкта доступу, що запросив програму (процес, завдання);

– результат запуску (успішний, неуспішний – несанкціонований).

4. Реєструвати спроби доступу програмних засобів (програм, процесів, завдань, задач) до захищуваних файлів. В параметрах реєстрації вказується:

– дата і час спроби доступу до захищуваного файлу з вказуванням її результату: (успішна, неуспішна - несанкціонована);

– ідентифікатор суб'єкта доступу;

– специфікація захищуваного файлу;

– ім'я програми (процесу, задачі, завдання), здійснюючих доступ до файлів;

– вид запрошуваної операції (читання, запис, видалення, виконання, розширення і тому подібне).

5. Реєструвати спроби доступу програмних засобів до наступних додаткових захищуваних об'єктів доступу: терміналам, ЕОМ, вузлам мережі ЕОМ, лініям (каналам) зв'язку, зовнішнім пристроям ЕОМ, програмам, томам, каталогам, файлам, записам, полям записів. В параметрах реєстрації вказується:

– дата і час спроби доступу до захищуваного файлу з вказуванням її результату (успішна, неуспішна – несанкціонована);

– ідентифікатор суб'єкта доступу;

– специфікація захищуваного об'єкту [логічне ім'я (номер)];

– ім'я програми (процесу, задачі, завдання), здійснюючих доступ до файлів;

– вид запрошуваної операції (читання, запис, монтування, захоплення і тому подібне).

6. Реєструвати зміни повноважень суб'єктів доступу, а також статусу об'єктів доступу. В параметрах реєстрації вказується:

– дата і час зміни повноважень;

– ідентифікатор суб'єкта доступу (адміністратора), який здійснює зміни.

7. Здійснювати автоматичний облік створюваних захищуваних файлів за допомогою їх додаткового маркування, використовуваного в підсистемі управління доступом. Маркування повинно відбивати рівень конфіденційності об'єкту.

8. Проводити облік усіх захищуваних носіїв інформації за допомогою їх маркування і із занесенням облікових даних в журнал (облікову картку).

9. Проводити облік захищуваних носіїв з реєстрацією їх видачі (прийому) в спеціальному журналі (картотеці).

10. Проводити декілька видів обліку (дублюючих) захищуваних носіїв інформації.

11. Здійснювати очищення (обнулення, знеособлення) областей оперативної пам'яті ЕОМ і звільнюваних зовнішніх накопичувачів. Причому очищення повинно здійснюватися двократним довільним записом в область пам'яті, що звільняється, раніше використану для зберігання захищуваних даних (файлів).

12. Сигналізувати про спроби порушення захисту.

Підсистема забезпечення цілісності повинна:

1. Забезпечувати цілісність програмних засобів СЗІ НСД, оброблюваної інформації, а також незмінність програмного середовища. При цьому:

– цілісність СЗІ НСД перевіряється при завантаженні системи по контрольним сумах компонент СЗІ;

– цілісність програмного середовища забезпечується використанням трансляторів з мови високого рівня і відсутністю засобів модифікації об'єктного коду програм в процесі обробки і (або) зберігання захищуваної інформації.

2. Здійснювати фізичну охорону ЗОТ (пристроїв і носіїв інформації). При цьому повинна передбачатися постійна наявність охорони на території будівлі і приміщень, де знаходиться АС. Охорона повинна проводитися за

допомогою технічних засобів охорони і спеціального персоналу, а також з використанням строгого пропускного режиму і спеціального устаткування в приміщенні АС.

3. Передбачати наявність адміністратора або цілої служби захисту інформації, відповідальних за ведення, нормальне функціонування і контроль роботи СЗІ НСД. Адміністратор повинен мати свій термінал і необхідні засоби оперативного контролю і дії на безпеку АС.

4. Проводити періодичне тестування функцій СЗІ НСД при зміні програмного середовища і персоналу АС за допомогою спеціальних програмних засобів не рідше одного разу в рік.

5. Мати в наявності засоби відновлення СЗІ НСД, які передбачають ведення двох копій програмних засобів СЗІ НСД і їх періодичне оновлення і контроль працездатності.

6. Використовувати тільки сертифіковані засоби захисту. Їх сертифікацію проводять спеціальні сертифікаційні центри або спеціалізовані підприємства, що мають ліцензію на проведення сертифікації засобів захисту СЗІ НСД.

1.1.4 Відмінності вимог і засадничих механізмів захисту від НСД

Порівняємо дві розглянуті вище групи вимог і їх особливості для захисту інформації різних категорій (конфіденційної і секретної).

Ясно, що ключовими механізмами захисту, що утворюють основну групу механізмів захисту від НСД (“Підсистема управління доступом”) являються:

– ідентифікація і перевірка достовірності суб'єктів доступу при вході в систему по ідентифікатору (коду) і паролю умовно-постійної дії;

– контроль доступу суб'єктів до захищуваних ресурсів відповідно до матриці доступу.

Додатковою вимогою і принциповою відмінністю при захисті секретної інформації є те, що механізмом захисту повинно здійснюватися управління

потоками інформації за допомогою міток конфіденційності. При цьому рівень конфіденційності накопичувача має бути не нижче рівня конфіденційності записуваної на нього інформації.

Всі три перераховані механізми є засадничими. Пов’язані вони таким чином: усі права доступу до ресурсів (розмежувальна політика доступу до ресурсів) задаються для конкретного суб’єкта доступу (користувача). Тому суб'єкт доступу (користувач) має бути ідентифікований при вході в систему, відповідно, має бути проконтрольована його достовірність. Зазвичай це робиться шляхом використання секретного слова - пароля.

Розглянемо механізми, що реалізовують основу захисту комп'ютерної інформації від НСД – розмежувальну політику доступу до ресурсів. Такими механізмами є механізми контролю доступу.

Наслідуючи формалізовані вимоги до системи захисту інформації, основу реалізації розмежувальної політики доступу до ресурсів при обробці відомостей конфіденційного характеру являється дискреційний механізм управління доступом. При цьому реалізується дискреційна модель доступу до ресурсів. При дискреційній моделі права доступу задаються матрицею доступу, елементами якої є дозволені права доступу суб'єкта до об'єкту. Що стосується контролю доступу, то він здійснюється безпосередньо шляхом аналізу прав доступу до об'єкту суб'єкта, що запрошує доступ. При цьому аналізується, чи є в матриці інформація про дозвіл доступу даного суб'єкта до цього об'єкту, чи ні.

При захисті секретної інформації в основі розмежувальної політики доступу (РПД) до ресурсів повинен лежати окрім дискреційного (дискреційна модель управління доступом), мандатний механізм керування доступом (мандатна модель управління доступом).

В рамках мандатного механізму кожному суб'єктові (користувачеві, застосуванню і так далі) і кожному об'єкту (файлу, каталогу і так далі) ставляться у відповідність спеціальні класифікаційні мітки. За допомогою цих міток суб'єктам і об'єктам призначаються класифікаційні рівні (рівні уразливості, категорії секретності і тому подібне), що є комбінаціями

ієрархічних і неієрархічних категорій. Сам контроль і управління доступом здійснюється шляхом зіставлення класифікаційних міток суб'єкта і об'єкта доступу, що відображають їх місце у відповідній ієрархії. В загальних рисах в цьому і полягає мандатний механізм керування доступом. Тобто право доступу надається на основі порівняння міток об'єкта і суб'єкта. При цьому, щоб суб'єкт отримав доступ до об'єкту, рівень конфіденційності має бути не нижчим рівня конфіденційності об'єкту.

Для системи захисту виконання вимоги “Має бути забезпечена цілісність програмних засобів системи захисту інформації від НСД (СЗІ НСД), оброблюваної інформації, а також замкнутість програмного середовища” забезпечує можливість протидії прихованим діям користувачів, спрямованих на отримання НСД до інформації в обхід РПД. При цьому не важливо, чим користуватиметься потенційний порушник – програмами власної розробки, всіма можливими налагоджувальними засобами або іншим ПЗ.

Вимога до очищення пам'яті “Повинно здійснюватися очищення (обнулення, знеусоблення) вивільнюваних областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів. Очищення здійснюється двократним довільним записом в область пам'яті, що звільняється, раніше використану для зберігання захищуваних даних обумовлює неможливість доступу користувача до залишкової інформації. Його необхідність викликана тим, що при видаленні файлу на зовнішньому накопичувачі системними засобами здійснюється зміна розмітки накопичувача, але власне інформація залишається. Вона так і називається "Залишкова інформація". При цьому з огляду на те, що остаточна інформація вже не є об'єктом доступу (вона відповідним чином не розмічена на диску - не є файлом), дискреційний і мандатний механізми контролю доступу не можуть здійснювати РПД до цієї інформації. А це означає, що доступ до неї може бути здійснений в обхід підсистеми управління доступом.

1.2 Об’єкти загроз

1.2.1 Класифікація загроз по способу їх здійснення

Розглянемо класифікацію загроз по способу їх здійснення. Ця класифікація нам потрібна для формування задач додаткового захисту інформації і приведена на рисунку 1.1.

Рисунок 1.1 – Класифікація загроз по способу їх здійснення

Явні загрози. Відповідно до даної класифікації загрози комп'ютерної безпеки поділимо на явні і приховані. Під явними розуміємо такі погрози, які зрозумілі і однозначно передбачені. Вони не вимагають для протидії їм будь-яких додаткових відомостей про статистику погроз і неочевидних припущень про можливі атаки зловмисника.

Явні погрози пов'язані з некоректною реалізацією і настройкою системи захисту. До таких можуть бути віднесені:

– некоректність реалізації механізму захисту;

– неповнота покриття каналів доступу до інформації механізмами захисту;

– некоректність (суперечність) можливих настройок механізмів захисту.

Прокоментуємо класифікацію явних погроз.

Некоректність реалізації механізму захисту може бути проілюстрована неможливістю в ОС Windows 9x/Me заборонити доступ до системного диска «на запис», а також неможливістю керувати доступом до не розділюваних системою і додатками каталогів (наприклад, «Temp», «Корзина», «Мої документи» і так далі). Це у свою чергу не дозволяє говорити про коректність реалізації механізму керування доступом до файлових об'єктів.

Якщо розглядати ОС Windows NT/2000/XP, то тут можна відзначити неможливість розмежувати доступ до пристроїв введення «на виконання», що дозволяє користувачеві запускати будь-які програми із зовнішніх носіїв.

Неповнота покриття каналів доступу до інформації механізмами захисту може бути проілюстрована неможливістю керування доступом до деяких ресурсів захищуваного об'єкту, наприклад, до віртуального каналу зв'язку і так далі. При цьому ресурси можуть бути як локальними, так і мережевими — в складі ЛОМ.

Некоректність (суперечність) можливих настройок механізмів захисту може розглядатися в двох аспектах: власне некоректність настройок і некоректність механізму (способу) задання настройок.

У першому випадку мова йде про неможливість для механізму захисту завдання коректних настройок як таких, наприклад, якщо для мандатного механізму керування доступом не реалізований принцип завдання настройок «все, що не дозволено, то заборонено».

В іншому випадку мова йде про настройку механізмів захисту в ієрархічній системі, де настройки може здійснювати адміністратор безпеки, адміністратор СУБД і додатку, користувач і так далі. Наприклад, користувач в ОС самостійно може розділяти (робити доступними з мережі) ресурси, до яких йому дозволений доступ, адміністратор СУБД може здійснювати настройки

вбудованих в СУБД механізмів захисту, а користувач самостійно може делегувати свою роль.

Приховані загрози. Під прихованими розуміємо такі погрози, які не очевидні, і вимагають для протидії їм додаткових припущень про можливі атаки зловмисника.

Приховані погрози пов'язані з нерегламентованими діями користувача перш за все за допомогою запуску власних програм, а також із використанням зловмисником помилок і закладок в системному і прикладному ПЗ.

При цьому прихована загроза може бути охарактеризована двома властивостями:

– характеристикою об'єкту загрози (наприклад, обліковий запис користувача);

– загальною характеристикою атаки зловмисника (наприклад, модифікація облікового запису із використанням власної запущеної програми. Дій подібної програми безліч, як відомих, так і невідомих).

З урахуванням сказаного можна зробити наступний найважливіший висновок: будь-який механізм захисту повинен проектуватися з урахуванням як явних, так і прихованих (у тому числі і невідомих) погроз інформаційної безпеки, оскільки тільки в цьому випадку можна говорити про можливість реалізації механізмом захисних властивостей.

1.2.2 Класифікація об’єктів загроз

Для обгрунтування структури системи захисту необхідно розглянути класифікацію об'єктів загроз. Вона представлена на рисунку 1.2.

З урахуванням цієї класифікації до об'єктів захисту можуть бути віднесені:

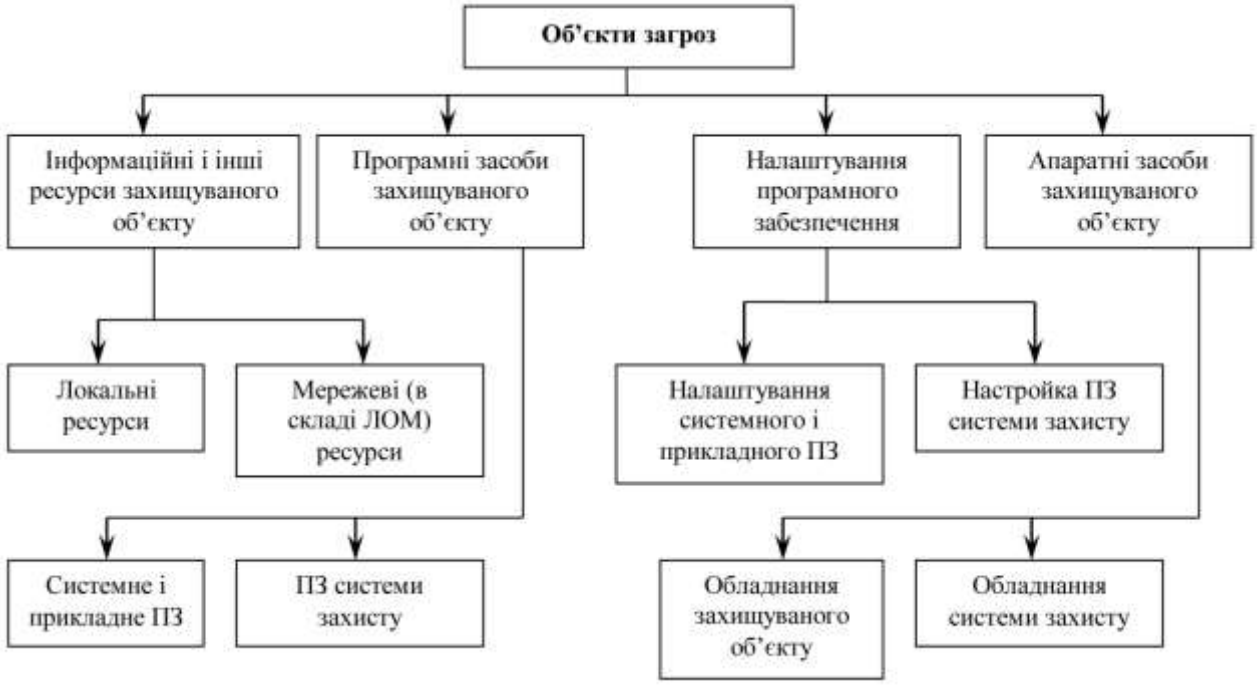

Рисунок 1.2 – Класифікація об'єктів загроз

1. Інформаційні і інші ресурси захищуваного об'єкту включаючи локальні і мережеві (у складі ЛОМ). До таких можуть бути віднесені власне система (вхід в систему), файлові об'єкти (локальні і розділювальні) і так далі.

2. Програмні засоби захищуваного об'єкту, включаючи програмні засоби ОС і додатків, а також ПЗ системи захисту. При цьому повинна бути забезпечена незмінність, а при необхідності — активність процесів, драйверів, динамічних бібліотек і так далі.

3. Настройки програмного забезпечення, включаючи настройки системного і прикладного ПЗ (реєстр ОС, файли настройок ОС і додатків, настройки BIOS і так далі), а також настройки системи захисту (файли настройок, реєстр ОС).

4. Апаратні засоби захищуваного об'єкту включаючи власне обладнання комп'ютера, а також обладнання системи захисту. При цьому з метою посилення захищеності може використовуватися додаткове обладнання, зокрема плата, що забезпечує функціональне розширення BIOS в частині введення пароля перед завантаженням системи із зовнішнього носія.

1.3 Функційна модель системи захисту

1.3.1 Основні групи механізмів захисту. Функційна модель

Сучасними нормативними документами в області захисту інформації в частині захисту від НСД [1, 2] виділяються наступні основні групи механізмів захисту:

1. Механізми авторизації користувачів.
2. Механізми управління доступом користувачів до ресурсів.
3. Механізми контролю цілісності.
4. Механізми реєстрації (аудиту).

Функціонально (з урахуванням дій користувача при доступі до ресурсів, а також з урахуванням протидії НСД до інформації механізмами захисту) система захисту повинна будуватися як ієрархічна система - можуть бути виділені декілька основних рівнів ієрархії захисту. Виділення даних рівнів і їх реалізація є необхідною (визначається формалізованими вимогами) умовою побудови системи захисту.

Функціональна модель системи захисту, яка може бути отримана на підставі аналізу формалізованих вимог до системи захисту, представлена на рисунку 1.3.

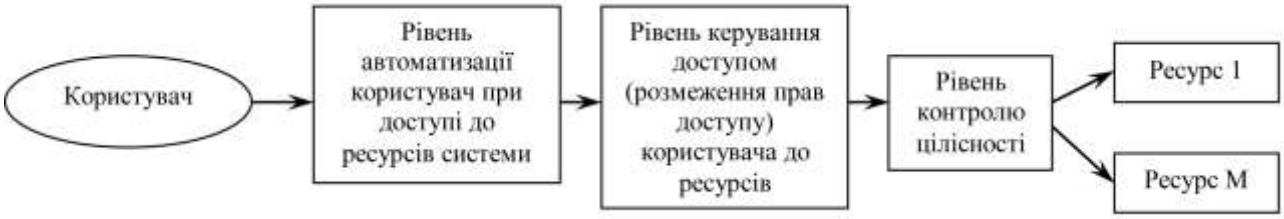

Рисунок 1.3 – Функціональна модель системи захисту інформації на основі формалізованих вимог

Функціональна модель системи додаткового захисту [9, 10, 12], яка вирішує розглянуті вище завдання, представлена на рисунку 1.4.

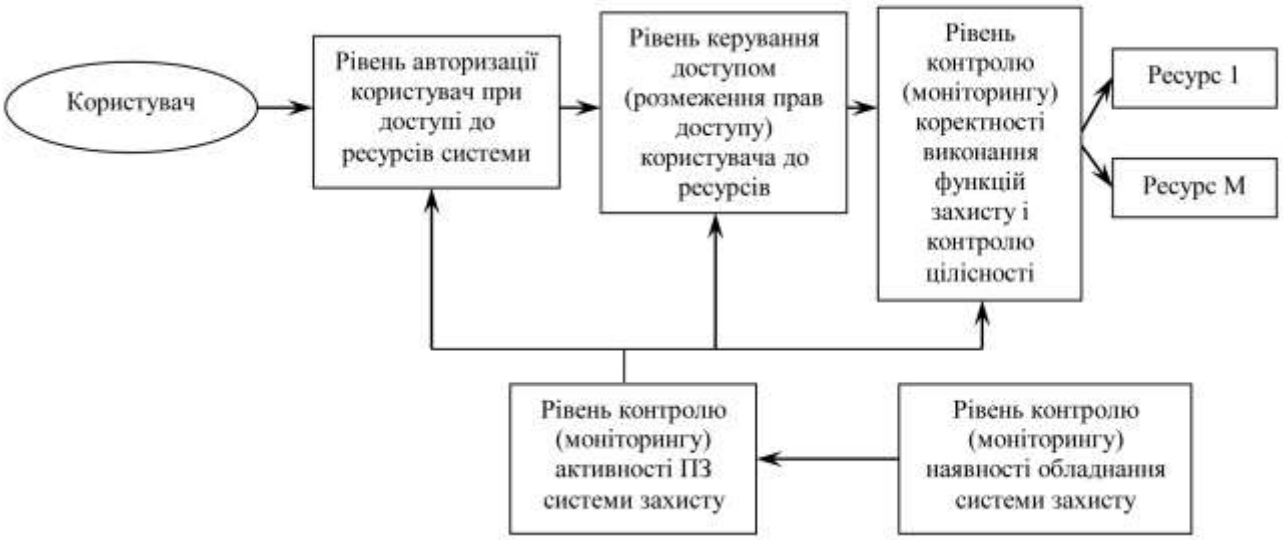

Рисунок 1.4 – Функціональна модель системи захисту інформації на основі розроблених вимог до додаткового захисту

З порівняння функціональних моделей, представлених на рис. 1.3 і рис. 1.4 видно, що з метою вирішення сформульованих вище завдань додаткового захисту в модель захисту включені:

– рівень контролю (моніторингу) активності ПЗ системи захисту;

– рівень контролю (моніторингу) наявності обладнання системи захисту;

– крім того, принципово змінені функції рівня контролю цілісності — даний рівень захисту тут функціонально призначений для контролю (моніторингу) коректності виконання функцій захисту і контролю цілісності.

Розглянемо призначення рівнів захисту в приведеній функціональній моделі. Задачі, що вирішуються на різних рівнях, реалізуються з урахуванням сформульованих для них вимог. При цьому кожен рівень захисту розглядатимемо як функціональний блок в представленій схемі.

Рівень авторизації користувача при доступі до ресурсів системи. Спершу треба визначитися, кого ми розумітимемо під користувачем. До користувачів, в рамках рівневої моделі захисту, можуть бути віднесені як користувачі додатків, які вирішують з використанням даного засобу відповідні

виробничі завдання, так і адміністратор безпеки, що є користувачем системи захисту.

Рівень авторизації користувача забезпечує перевірку облікових параметрів користувача при доступі в систему і до системи захисту. Також цим рівнем захисту вирішується ряд допоміжних завдань, наприклад, запуск процесу (застосування) після авторизації відповідальної особи і ін.

Рівень керування доступом (розмежування прав доступу) користувача до ресурсів. Рівень керування доступом (розмежування прав доступу) реалізує власне розмежувальну схему доступу користувачів до ресурсів захищуваного об'єкту, а також політика адміністрування системи захисту в рамках виконання політики інформаційної безпеки. Під системою захисту тут розуміємо відповідні механізми, вбудовані до ОС, СУБД, додатків, а також додаткових механізмів захисту.

Для вирішення задачі управління доступом до ресурсів на цьому рівні виділяються локальні і мережеві ресурси. До локальних ресурсів, що вимагають розмежування доступу користувачів, відносяться:

– файлові об'єкти (логічні диски, каталоги, файли);

– пристрої із змінними носіями (зокрема, дисковод і CD-ROM);

– відчужувані фізичні носії інформації (зокрема дискети і CD-ROM диски);

– комунікаційні порти;

– локальні принтери;

– процеси (виконувані файли), зокрема процеси ОС, системи захисту і застосувань — в частині їх модифікації і запуску;

– настройки ОС (для ОС Windows — реєстр ОС);

– файли настройок системи захисту;

– файли настройок застосувань;

– при використанні СУБД — таблиці даних і таблиці настройок;

– настройки «робочого столу» ОС і так далі.

До мережевих ресурсів (у складі ЛОМ), що вимагають розмежування доступу користувачів, відносяться:

– мережеві ресурси (по протоколу NetBios для мережі Microsoft), що розділяються, до яких відносяться файлові об'єкти, що розділяються, пристрої із змінними носіями (віртуальні канали зв'язку мережі Microsoft);

– мережеві ресурси, наприклад, по протоколу TCP/IP (хости, протоколи), віртуальні канали зв'язку мережі TCP/IP;

– мережеві принтери; мережеві служби і застосування (зокрема застосування інформаційних систем, наприклад, СУБД), в частині їх модифікації і запуску;

– файли настройок мережевих служб і застосувань і так далі.

Розмежувальна політика розглядається як у вигляді розмежування доступу до ресурсів, так і у вигляді функцій, що реалізовують дозволений доступ (наприклад, читання, запис, виконання і ін.). Вирішення задач розмежування доступу користувачів до ресурсів припускає і реалізацію процедур повернення колективно використовуваного ресурсу в початковий стан для його надання іншому користувачеві (наприклад, очищення оперативної і зовнішньої пам'яті).

На цьому рівні також вирішується задача розподілу функцій адміністрування безпекою системи між користувачами, системним (мережевим) адміністратором, адміністраторами СУБД і застосувань, адміністратором безпеки. При цьому вирішується задача централізації схеми адміністрування безпеки, в рамках якої зміна настройок безпеки на різних рівнях ієрархії системи повинна здійснюватися тільки при безпосередньому контролі з боку адміністратора безпеки.

Рівень контролю (моніторингу) коректності виконання функцій захисту і контролю цілісностю. Відзначимо, що сама по собі задача контролю цілісності припускає можливість несанкціонованого доступу до інформації (інакше достатньо перших двох рівнів захисту). Таким чином, даний механізм апріорі служить протидії прихованим погрозам в припущенні, що

зловмисником подолано перші два рівні захисту, які реалізують розмежувальну політику доступу до ресурсів захищуваного об'єкту.

В рамках формалізованих вимог недолік механізму контролю цілісності полягає в тому, що даний механізм, по-перше, реалізує дуже обмежений набір функцій, а по-друге, не дозволяє забезпечувати ефективну реакцію на приховану атаку в реальному часі. По суті він тільки фіксує її факт і наслідки.

З урахуванням сказаного функціональні завдання цього рівня захисту має сенс принципово розширити. При цьому до вже існуючих задач контролю доцільно додати контроль (моніторинг) коректності виконання розмежувальної політики доступу, що реалізовується на попередньому рівні. Зокрема на цьому рівні слід в реальному часі фіксувати факти використання зловмисником помилок і закладок в системному і прикладному ПЗ, а також надавати протидію даній групі прихованих погроз. До цього рівня також слід віднести контроль цілісності програм і даних, тобто контроль об'єктів файлової системи.

На відміну від двох попередніх рівнів, де відповідні механізми (програмні модулі системи захисту) запускаються асихронно за фактом запиту в системі на доступ до ресурсу, даний рівень реалізує синхронну процедуру контролю. При цьому він контролює відповідні події періодично, що пов'язано з його сильнішим впливом на завантаження обчислювального ресурсу захищуваного об'єкту в порівнянні із більшістю механізмів захисту двох попередніх рівнів.

Виняток становлять механізми розподілу функцій адміністрування безпекою системи, що лише реалізовуються на попередньому рівні, між користувачами, системним (мережевим) адміністратором, адміністраторами СУБД і додактів, а також адміністратором безпеки. Ці механізми також реалізуються з використанням синхронної процедури контролю.

Рівень контролю (моніторингу) активності системи захисту. Очевидно, що більшість задач захисту інформації вирішуються програмно, тобто захищеність комп'ютерної інформації забезпечується до тих пір, поки активне ПЗ системи захисту. При цьому включення в систему механізмів

додаткового захисту, які можуть бути реалізовані на різних рівнях (як на системному, так і на прикладному), пов'язано з появою додаткової групи погроз — погроз завантаження системи без механізмів додаткового захисту і погроз перекладу механізмів захисту в пасивний стан (відключення) в процесі функціонування захищуваного об'єкту.

В задачі даного рівня входить контроль активності системи захисту, із запобіганням можливості функціонування системи в незахищеному стані. Останнє може бути пов'язане як з можливістю завантаження ОС без системи захисту (або із урізаними функціями), так і з можливістю переходу системи захисту, або її компонент, в пасивний стан в процесі функціонування захищуваного об'єкту.

Очевидно, що активність однієї програми не має сенсу контролювати іншою програмою, запущеною на тому ж комп'ютері. Тому в рамках даного рівня повинні бути реалізовані наступні дві можливості аналізу активності системи захисту:

- локальна — з використанням апаратної компоненти (плати);
- мережева — віддалено, адміністратором з сервера безпеки.

При реалізації даного рівня захисту повинна здійснюватись протидія як явним, так і прихованим погрозам.

Рівень контролю (моніторингу) наявності обладнання системи захисту. Даний рівень захисту доцільно реалізовувати в тому випадку, якщо система захисту містить апаратну складову. При цьому захист від загрози видалення апаратної компоненти, крім організаційних заходів, може забезпечуватися технічними засобами.

Спочатку даний рівень забезпечує технічний захист від загрози видалення апаратної компоненти системи захисту. Проте його реалізація дозволяє комплексувати в єдиній технічній системі захисту інформації різні функції захисту: захисту комп'ютерної інформації, контролю доступу в приміщення, протипожежній безпеці і так далі. Причому все це буде доступно з єдиного робочого місця адміністратора.

1.3.2 Рекомендації по окремим рівням функціональної моделі.

З урахуванням вищенаведеного можемо зробити наступні висновки:

1. При побудові системи додаткового захисту інформації доцільно принципово переглянути функції рівня контролю цілісності. Позиціонуватимемо даний рівень захисту, як рівень контролю (моніторингу) коректності виконання функцій захисту і контролю цілісності.

2. У рівневу функціональну модель захисту має сенс включити рівень контролю (моніторингу) активності системи захисту, а при використанні апаратної компоненти захисту функціональна модель може бути доповнена рівнем контролю (моніторингу) наявності обладнання системи захисту.

3. Рівні ж авторизації користувача і управління доступом повинні забезпечувати вирішення задач коректності і повноти розмежувань доступу користувача до ресурсів. Крім того, повинна бути реалізована також можливість протидії групі прихованих погроз, пов'язаних з нерегламентованими діями користувача.

1.4 Критерії оцінки захисту комп'ютера

Критерії оцінки захисту комп'ютера (англ. Trusted Computer System Evaluation Criteria, TCSEC) - стандарт Міністерства оборони США, що встановлює базові вимоги щодо контролю комп'ютерної безпеки вбудованої в обчислювальну систему. TCSEC використовався, щоб оцінювати, класифікувати та обирати комп'ютерні системи, які використовуються для обробки, зберігання та надання доступу до класифікованої інформації.

На TCSEC, часто посилаються як на Оранжеву книгу, яка є основною в серії "веселкових пулікацій". Перше видання було зроблене в 1983 Національним центром комп'ютерної безпеки (NCSC). Пізніше перевидана у 1985. TCSEC було замінено у 2005 на міжнародний стандарт.

Класи захисту.

За допомогою критеріїв оцінки гарантовано захищених обчислювальних систем можна визначити сім класів захисту систем.

Клас D. Мінімальний захист (англ. Minimal protection). Цей клас зарезервований для тих систем, що були піддані оцінці, але в яких не вдалося досягти виконання вимог більш високих класів оцінок.

Клас C1. Вибіркового захисту (англ. Discretionary protection) Гарантовано захищена обчислювальна база (ТСВ) систем класу С1 забезпечує поділ користувачів і даних. Вона містить засоби управління, здатні реалізувати обмеження до доступу, щоб захистити проект або приватну інформацію і не дати іншим користувачам випадково читати або руйнувати їх дані. Передбачається, що середовище класу С1 є таким середовищем, у якому можуть кооперуватися користувачі, що обробляють дані, які належать до того самого рівня секретності.

Клас C2. Захист, заснований на керованому контролі доступом. Всі вимоги до класу С1 переносяться на клас С2. Крім того, системи цього класу реалізують структурно більш «тонке» управління доступом порівняно із системами класу С1 за рахунок додаткових засобів управління розмежуванням доступу і поширенням прав, а також за рахунок системи реєстрації подій (аудит), що мають відношення до безпеки системи і поділу ресурсів. Спеціально вводиться вимога щодо «очищення» ресурсів системи при повторному використанні іншими процесами.

Клас B1. Мандатний захист, заснований на присвоюванні міток об'єктам і суб'єктам, що перебувають під контролем ТСВ. Вимоги для систем класу В1 припускають виконання усіх вимог, які були необхідні в класі С2. Крім цього, необхідно навести неформальне визначення моделі, на якій будується політика безпеки, присвоювання міток даним і мандатним управлінням доступом іменованих суб'єктів до об'єктів. В системі необхідно мати засіб, що дозволяє точно і надійно присвоювати мітки експортованої інформації.

Клас B2. Структурований захист. Усі вимоги класу В1 мають виконуватися для системи класу В2. В системах класу В2 ТСВ заснована на

чітко визначеній і формально задокументованій моделі, в якій управління доступом поширюється на всі суб'єкти й об'єкти даної системи автоматичної обробки даних. Крім цього, має бути проведений аналіз, пов'язаний із наявністю побічних каналів витоків. Необхідно провести розбивку структури ТСВ як за критичними із погляду захисту елементами, так і за некритичними. Інтерфейс ТСВ добре визначений, а її проект і реалізація виконані так, що вони дозволяють проводити ретельне тестування і повний аналіз. Механізми аутентифікації посилені, управління захистом передбачається у вигляді засобів, що призначаються для адміністратора системи і для оператора, а на управління конфігурацією накладаються жорсткі обмеження. Система відносно стійка до спроб проникнення в неї.

Клас В3. Домени безпеки. Усі вимоги для систем класу В2 включені у вимоги до систем класу В3. ТСВ класу В3 має реалізовувати концепцію монітора звертань, гарантовано захищеного від несанкціонованих змін, пошкодження і підробки, який обробляє всі звертання. Передбачається введення адміністратора безпеки системи, механізми контролю (аудит) розширені так, щоб забезпечити обов'язкову сигналізацію про всі події, пов'язані з можливим порушенням встановлених у системі правил безпеки. Обов'язковою також є наявність процедур, що забезпечують відновлення працездатності системи. Система даного класу найвищою мірою стійка відносно спроб проникнення в неї.

Клас А1. Верифіковоний проект. Системи цього класу А1 функціонально еквівалентні системам класу В3 у тому відношенні, що і них не з'являються будь-які нові вимоги до політики забезпечення безпеки. Характерна риса систем даного класу — формальна специфікація проекту; і верифікації захисту, тобто високий ступінь впевненості в тому, що гарантовано захищена обчислювальна база реалізована правильно.

1.5 Критерії оцінки інформаційної безпеки

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Для характеристики основних критеріїв інформаційної безпеки застосовують модель тріади CIA (en:CIA_Triad).

Ця система передбачає такі основні характеристики інформаційної безпеки:

- конфіденційність,
- цілісність,
- доступність (англ. Confidentiality, Integrity and Availability (CIA)).

Інформаційні системи аналізуються в трьох головних секторах: технічних засобах, програмному забезпеченні і комунікаціях, з метою ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання, на трьох рівнях або шарах: фізичний, особистий і організаційний. По суті, процедури або правила запроваджуються для інформування адміністраторів, користувачів та операторів щодо використовування захисних продукцію для гарантування інформаційної безпеки в межах організацій.

Нормативний документ ТЗІ 2.5-004-99. В Україні також розробляються і використовуються критерії інформаційної безпеки. Наприклад департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» який подібний до моделі тріади CIA.

Функціональні критерії.

Складові інформаційної безпеки або властивості: конфіденційність (англ. Confidentiality, privacy), цілісність (англ. Integrity), доступність (англ. Availability) — тріада CIA.

Функціональні критерії розбиті на чотири групи вимог захисту проти певних типів загроз:

– конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги відносяться до критеріїв конфіденційності. Є 5 головних послуг;

– цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку, якщо існують вимоги щодо обмеження можливості модифікації інформації, то їх відносяться до критеріїв цілісності.

– доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то їх відносяться до критеріїв доступності;

– спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні функції відносяться до критеріїв спостереженості;

Критерій гарантій.

Окрім функціональних критеріїв захищеності існують таки критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

Міжнародний стандарт ISO/IEC 15408.

Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) описує інфраструктуру (Framework) в якій користувачі комп'ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цей стандарт дозволяє бути впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку. Прообразом даного документа послужили «Критерії оцінки безпеки інформаційних технологій» (англ. Evaluation Criteria for IT Security, ECITS), робота над якими почалася в 1990 році.

Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізує їх механізмів, і вимоги довіри, які пред'являються до технології та процесу розробки та експлуатації.

1.6 Висновки до першого розділу

В розділі розглянуто основи систем захисту інформації.

Загрози комп'ютерної безпеки діляться на явні і приховані. Під явними розуміємо такі погрози, які зрозумілі і однозначно передбачені. Вони не вимагають для протидії їм будь-яких додаткових відомостей про статистику погроз і неочевидних припущень про можливі атаки зловмисника.

Критерії оцінки захисту комп'ютера встановлюють базові вимоги щодо контролю комп'ютерної безпеки вбудованої в обчислювальну систему, використовуються, щоб оцінювати, класифікувати та обирати комп'ютерні системи, які використовуються для обробки, зберігання та надання доступу до класифікованої інформації.

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

2 СЕРВЕРИ SUN MICROSYSTEMS

Компанія Sun грає головну роль в сегменті серверів Інтернету, вона також займає провідні позиції в розробці сховищ даних, а саме: проводить апаратні засоби, ПЗ, забезпечуючи можливості стратегічної консолі управління для системних мереж (SAN) і інших систем сховищ даних. Протягом останніх декількох років компанія запропонувала декілька промислових стандартів, таких як тести TPC-C (тести для оцінки продуктивності комп'ютера і співвідношення ціна/продуктивність), які можуть застосовуватися для великих систем баз даних, таких як Oracle, DB2, SQL Server і так далі, розгорнутих на промислових серверах [56].

2.1 Сервери і процесори SPARC

В середині 1980-х років на ринку з'явилася лінійка робочих станцій Unix, що працюють під управлінням ОС Sun на основі версії Unix, під назвою Berkeley Software Distribution. Ці станції отримали високі оцінки споживачів. Починаючи з 1982 року на серверах Sun встановлюється набір протоколів TCP/IP. До 1985 року компанія Sun заснувала свою організацію провайдерів послуг Інтернету (IPO), а до 1987 року вона перетворилася на промислового лідера на ринку робочих станцій. На той час ця компанія випускала самі швидкодіючі і успішно продавані пристрої, представлені на ринку апаратного забезпечення.

У 1988 році фахівці з компанії Sun створили робочу станцію SPARCstation 1, корпус якої нагадував коробку з-під піци (так званий дизайн "pizza box"). В певній мірі 1991 рік було переломним моментом для компанії. Цього року Sun представила операційну систему Solaris 2 для процесорів RISC - призначену для систем симетричної мультипроцесорної обробки (SMP). Робоча станція SPARCstation 10, що з'явилася в 1992 році, була першою настільною системою з можливостями симетричної мультипроцесорної обробки. У цьому ж

році Sun поставила на ринок найбільшу кількість RISC-систем в порівнянні з будь-якими іншими виробниками Unix –систем [56].

Зростання популярності Інтернету сприяло подальшому просуванню компанії Sun в сегменті виробників серверів. Інтернет-провайдерам для організації своїх мереж вимагалися маршрутизатори, комутатори і брандмауери, і усі ці пристрої надавались компанією Sun. Вибираючи устаткування відповідно до критерію "ціна/продуктивність", багато користувачів віддавали перевагу серверам Sun через їх конкурентну ціну. Через зростанням ринку Інтернет-устаткування робочі станції Sun, а пізніше і сервери Sun стали основною платформою не лише для маршрутизаторів, але і для веб-серверів і інших серверів застосувань. З часом компанія Cisco потіснила Sun на ринку маршрутизаторів, але в сегменті Інтернет-серверів пристроям компанії Sun немає рівних.

У 1996 році компанія Sun представила системи UltraSPARC, засновані на її першому 64-розрядному процесорі. У цьому ж році увазі користувачів була представлена мова Java і розробки в області XML цієї ж компанії. Рік потому компанія представила свою першу високорівневу серверну систему, Sun Enterprise 10000, яка насправді являлась системою класу "мейнфрейм". Ця система встановила рекорди продуктивності по тестах TCP-C для усіх провідних баз даних. Окрім серверів, компанія Sun почала випускати менш потужні системи, призначені для використання як "будівельні блоки" при розгортанні горизонтально масштабованих застосувань, таких як сервери Netra tl і корпоративні пристрої Sun Ray 1 (у 1999 році) і системи класу "мідфрейм", Sun Fire, - в 2001 році [56].

Усі сервери, що випускалися компанією Sun до 2002 року, використовували виключно процесори RISC і працювали під управлінням ОС Solaris, поки не з'явився універсальний сервер Sun LX50, який міг працювати під управлінням ОС Solaris або Linux. У 2002 році з'явився сервер, побудований на основі архітектури N1, що працює за принципом "мережа – це комп’ютер", а в 2003 році компанія Sun почала освоювати сегмент мережевих обчислень. При

виконанні обчислень цього роду для вирішення одного і того ж завдання використовується декілька мережевих комп'ютерів.

2.1.1 Архітектура RISC

Зараз існують два підходи до розробки комп'ютерних процесорів: архітектура CISC і архітектура RISC. В даному випадку йдеться швидше не про конструктивне рішення конкретного процесора, а про філософські принципи, на основі яких виконується розробка процесора. CISC-процесор має розширений набір команд, і вони можуть бути складнішими, ніж ті ж самі команди в RISC-процесорі. Особливість CISC-команд полягає в тому, що їх виконання може займати декілька циклів процесора.

У 1970-х роках, коли розробники процесорів вирішили детально ознайомитися з командами, які найчастіше використовуються в програмах на мовах асемблера, вони дійшли висновку про те, що найчастіше застосовуються прості команди. Навіть складні команди часто представляються у вигляді простіших команд. Широко відомий приклад цьому – команда VAX INDEX, яка, як з'ясувалося, виконувалася повільніше, ніж набір простіших команд, що генерують аналогічні структури даних, що імітує її. Після цього були зроблені відповідні висновки, і в результаті складні команди, названі ортогональними режимами адресації, ігнорувалися, а додаткові команди конвертувалися компіляторами. У результаті зникла потреба в створенні програм на мові асемблера. На сьогодні компіляція коду - це стандартний крок, що виконується до запуску програми на виконання [57].

Розробники RISC-процесорів використовують менший набір команд в порівнянні з CISC-процесорами, але вони прагнуть оптимізувати ці команди так, щоб обчислення були ефективнішими. Команда в CISC-процесорі, яка могла б бути комбінацією чотирьох простіших команд і займати вісім циклів процесора при виконанні на RISC-процесорі, перетворюється на чотири окремі команди, які, як і раніше, виконуються упродовж восьми циклів процесора, але оскільки команди менші за розміром, то процес їх обробки ефективніший через

меншу кількість "втрачених" циклів. Саме у цьому полягають відмінності між цими двома типами процесорів (принаймні, теоретично).

RISC-процесори пропонують декілька додаткових переваг, завдяки яким вони так часто застосовуються при створенні високопродуктивних систем. По-перше, спрощується конструкція самого процесора внаслідок використання меншого набору команд. Спрощена конструкція означає, що процесор може бути дешевшим або мати додаткові характеристики в порівнянні із складнішим процесором. Завдяки зменшеному набору команд для їх зберігання вимагається менший об'єм пам'яті. При умові, що центральні процесори працюють набагато швидше, ніж мікросхеми пам'яті, мень-ший об'єм пам'яті - це дуже бажана характеристика.

Нижче перераховані основні властивості RISC -процесорів.

– Великий розмір внутрішньої кеш-пам'яті.

– Додаткові регістри, які є однорідніші, ніж регістри CISC-процесора.

– Вбудований пристрій управління вводом-виводом і таймери, доступні в застосуваннях контролерів.

– Характеристики наступного покоління процесорів, реалізовані із застосуванням традиційних дизайнерських рішень. Завдяки цьому можна використовувати колишнє виробниче устаткування для створення нового серійного процесора.

– Вбудовані графічні процедури.

– Паралелізм, реалізований за допомогою конвеєрної обробки або суперскалярних обчислень.

– Виключення деяких характеристик в цілях зменшення енергоспоживання процесорів.

Прикладами центральних процесорів з RISC-архітектурою являються Sun SPARC і UltraSPARC, IBM PowerPC, MIPS, а також процесори DEC Alpha.

Ще одна додаткова перевага RISC в тому, що в них простіше реалізуються швидкісні внутрішні шини даних (в порівнянні з CISC-процесорами). Завдяки цьому прискорюється передача невеликих фрагментів даних, які генеруються в процесі роботи RISC-процесора. У кінці 1990-х років розрядність внутрішніх шин даних цих процесорів збільшилася до 64. Використовуючи шини з більшою розрядністю, можна також добитися вищої ефективності процесора при роботі на нижчих частотах, що сприятиме зниженню тепловиділення. Завдяки можливостям RISC-процесорів також спростилося створення ефективно працюючих компіляторів - програм, які перетворюють програмні коди в команди, які "розуміє" процесор [57].

З усього вищесказаного можна зробити висновки про те, що архітектура RISC має неоспоримі переваги і повинна використовуватися повсюдно. Але не поспішатимемо з висновками. Використовуючи архітектуру CISC, розробники дістають можливість використання багатшого середовища розробки, що полегшує створення програм. Важливу роль грає тривала історія розвитку цієї архітектури, упродовж якої були впроваджені ряд поліпшень і удосконалень. Найяскравіший приклад реалізації CISC-архітектури - це всім відомі процесори сімейства Intel x86. Починаючи з Pentium Pro, компанія Intel почала впроваджувати RISC-властивості у свої центральні процесори. Зараз технології, використовувані при розробках процесорів цього сімейства, – гібрид архітектури CISC і RISC. Наведене відноситься і до ряду процесорів, пропонованих іншими розробниками.

В міру розвитку технології стало неможливим стверджувати, що цей процесор є “чистим” CISC-процесором, а інший процесор – “чистим” RISC–процесором. Набори команд RISC-процесорів були істотно розширені, а в CISC-процесорах з'явилися типові властивості RISC-процесорів. Виробники процесорів оптимізують застосовувані технології, внаслідок чого стало можливим впровадження RISC-характеристик в CISC- процесорах, а CISC-характеристик – в RISC-процесорах. Тому складно однозначно стверджувати, яка архітектура краща.

2.1.2 Процесори SPARC і UltraSPARC

Процесор SPARC став логічним наслідком розробки RISC-процесора, выполняв-шейся в Беркли на початку 1980-х років. Абревіатура SPARC розшифровується як Scalable Processor Architecture (масштабована архітектура процесора), і хоча термін SPARC не-вільно асоціюється з компанією Sun Microsystems, насправді це зареєстрована торговельна марка компанії SPARC International, Inc. Ця компанія просуває SPARC як відкриту системну архітектуру. Тому на ринку представлені SPARC-процесори, розроблені не лише компанією Sun, але і Cypress Semiconductor, Fujitsu, Texas Instruments, а також компанією Gaiser.

В процесорах архітектури SPARC використовується зворотний порядок байт, на відміну від процесорів архітектури x86, які засновані на прямому порядку байт. Саме з цієї причини неможливо перекомпілювати програму, написану для процесора x86, в програму для процесора SPARC, і навпаки. В цьому випадку доведеться повністю переписувати саму програму.

Одна з самих легко впізнанних характеристик SPARC-процесорів, яка зближує їх з RISC-процесорами, – це порядок використання регістрів загального призначення, РОН (GPR). Процесор SPARC може адресувати до 128 регістрів загального призначення, з яких 8 призначені для глобального використання, а 24 формують вікно регістра, яке можна використовувати для викликів функції в стеку регістра. Регістрове вікно, що включає 8 локальних регістрів, спільно використовує їх з регістровими вікнами, що знаходяться поруч. Спільно використовувані (чи спільні) регістри передають параметри і встановлюють значення, тоді як локальні регістри зберігають значення, використовувані при багатократних викликах функції. Програми, написані з урахуванням використання SPARC-архітектури, звертаються лише до 32 регістрів (8+24). Ця архітектура називається масштабованою, оскільки програми можуть використовувати 32 регістрові вікна, декілька таких вікон або одне з них. При використанні більшої кількості вікон відбувається частіше контекстне переключення, потрібне для завантаження/вивантаження сторінок

пам'яті з інструкціями, але при цьому в пам'ять завантажується більша кількість інструкцій.

У таблиці 2.1 приведені основні характеристики різних поколінь процесорів SPARC.

Таблиця 2.1 – Серійні процесори SPARC

Модель	Тактова частота, МГц	Рік випуску	Процес, нм	Кількість транзисторів, млн.	Розмір, мм кв.
Версія 8					
microSPARC I	50	1992	0,8	0,8	225
SuperSPARC I	33-65	1992	0,8	3,1	н/д
microSPARC II	60-125	1992	0,5	2,3	233
SuperSPARC II	75-90	1994	0,8	3,1	299
TurboSPARC I	60-180	1995	0,35	н/д	н/д
Версія 9					
UltraSPARC I	140-200	1995	0,5	5,2	315
UltraSPARC II	250-480	1997	0,25	5,4	156
UltraSPARC III	270-480	1998	0,25	5,4	148
UltraSPARC IIe	400-500	2000	0,18 Алюміній	н/д	н/д
UltraSPARC III+	550-650	2002	0,18 Мідь	н/д	н/д
UltraSPARC III	600-1200	2001	0,13	29	330
UltraSPARC IIIi	1064-1593	2003	0,13	87,5	206
UltraSPARC IV	1050-1350	2004	0,13	66	356

Продовження таблиці 2.1

Модель	Кількість контактів	Потужність, Вт	Напруга, В	Кеш даних, Кбайт	Кеш команд, Кбайт	Об'єм кеш пам'яті, Кбайт
Версія 8						
microSPARC I	288	2,5	5	4	2	0
SuperSPARC I	н/д	14,3	5	16	20	1,024
microSPARC II	321	5	3,3	8	16	0
SuperSPARC II	н/д	16	н/д	16	20	2,048
TurboSPARC I	416	7	3,5	16	16	1,024
Версія 9						
UltraSPARC I	521	30	3,3	16	16	1,024
UltraSPARC II	521	21	3,3	16	16	8,192
UltraSPARC III	587	21	1,9	16	16	2,048
UltraSPARC IIe	370	13	1,7	16	16	256
UltraSPARC III+	370	17,6	1,7	16	16	512
UltraSPARC III	1368	53	1,6	64	32	8,192
UltraSPARC IIIi	959	52	1,3	64	32	16,384
UltraSPARC IV	1368	108	1,35	64	32	16,384

Новітні версії процесорів SPARC мають номери 8 і 9. Процесор версії 8 включає 16 регістрів з плаваючою комою подвоєної точності, причому кожен з них може застосовуватися по-різному. Цей регістр можна використовувати для зберігання двох значень з одинарною точністю, внаслідок чого досягається ефект застосування 32 регістрів з одинарною точністю. Можна також об'єднати парний і непарний регістр з подвоєною точністю, що дозволяє створювати до 8 регістрів із збільшеною учетверо точністю. Як альтернативу можна використовувати 32 регістри як стандартні регістри з подвоєною точністю [58].

Процесор SPARC версії 9 примітний тим, що це була перша 64-розрядна модель. У цьому процесорі з'явилися 16 додаткових регістрів з подвоєною точністю, які були додані до архітектури в цілях підтримки внутрішньої 64-розрядної шини даних. Звичайно ж, навіть якщо процесор працюватиме з внутрішньою 64-розрядною шиною, системна шина вводу-виводу все ще має 32-розрядну архітектуру. Існує безліч прикладів систем, що працюють на 64-

розрядній внутрішній шині центрального процесора і 32-розрядній шині вводу-виводу, як і в протилежному випадку з 32-розрядною шиною центрального процесора поверх 64-розрядної шини вводу-виводу.

2.2 Категорії серверів

2.2.1 Сервери початкового рівня

Сервер початкового рівня – це звичайно універсальний сервер. В порівнянні з іншими виробниками сервери початкового рівня компанії Sun підтримують найбільшу кількість операційних систем. Ці сервери побудовані на основі процесорів Opteron і UltraSPARC (серія III і IIIi). Процесори Opteron можуть виконувати не лише операційні системи Solaris, але і Linux, Windows і VMware. Для багатьох споживачів сервери початкового рівня компанії Sun – це економічна платформа, яка може застосовуватися для горизонтального масштабування застосувань.

Всі сервери початкового рівня компанії Sun відносяться до серії Sun Fire. Єдине виключення - iForce VPN Firewall Appliance. Відмітною ознакою цих серверів є те, що вони встановлюються на стійках, є низькопрофільними, а їх розміри варіюються від 1 до 4U. Сервери початкового рівня Sun позиціонуються для Інтернет-ринку. Ці стійкові сервери призначені для реалізації горизонтально масштабованих застосувань, таких як ферми серверів, використовуваних для розгортання веб-сайтів.

Сервери початкового рівня Sun бувають різними – в основному одно- і двопроцесорні системи, хоча є і восьмипроцесорний сервер 4U Sun Fire V880. (Цю модель складно віднести до початкового рівня, хоча вона відноситься саме до цієї категорії.) В таблиці 2.2 приводяться деякі основні характеристики сучасних моделей серверів початкового рівня серії Sun Fire [59] .

Таблиця 2.2 – Серія серверів початкового рівня Sun Fire

Модель	Центральні процесори	Тактова частота	Версія операційної системи
Sun Fire V20z	1-2 процесори AMD Opteron 200	Моделі 244, 248, 250, 252	Solaris OS, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows або VMware
Sun Fire V40z	2-4 дво- одноядерні процесори AMD Opteron 800	Моделі 844, 858, 850, 852, 875	ОС Solaris, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows або Vmware
Sun Fire V100	1 процесор UltraSPARC III	550 МГц – 650 МГц	Solaris 8 (оновлення 2/02 і новіший), Solaris 9
Sun Fire V120	1 процесор UltraSPARC III	650 МГц	Solaris 8 (оновлення 10/01 і новіший), Solaris 9
Sun Fire V210	1-2 процесори UltraSPARC III	1,34 ГГц	Solaris 8 (варіант виконання для апаратних засобів 12/02 і новіший), Solaris 9 (оновлення 04/03 і новіше)
Sun Fire V240	1-2 процесори UltraSPARC IIIi	1 ГГц або 1,134/1,5 ГГц	Solaris 8 (варіант виконання для апаратних засобів 12/02 і новіший), Solaris 9 (оновлення 04/03 і новіше)
Sun Fire V440	2-4 процесори UltraSPARC III	1,28 ГГц або 1,593 ГГц	Solaris 8 (варіант виконання для апаратних засобів 7/03) і Solaris 9 (оновлення 12/03 і новіше)
Sun Fire V480	2-4 процесори UltraSPARC III, мідь	1,05 ГГц або 1,2 ГГц	Solaris 8, Solaris 9
Sun Fire V880	2-8 процесорів UltraSPARC III	1,2 ГГц	Solaris 8 (оновлення 10/01 і новіше), Solaris 9

У 2004 році з'явилася лінійка базових серверів, розроблена на основі лінійки серверів Qube. Разом з лінійкою пристроїв Cobalt і базовими кешуючими серверами лише одна з цих систем залишилася на плаву після фінансової кризи. З усіх цих систем лише станція Sun Control Station має перспективи подальшого розвитку, а лінійка базових серверів Sun виродилась в стратегію, засновану на застосуванні програмних засобів, і кращим

підтвердженням цьому являється пакет iForce VPN, який може виконуватися на різних системах.

Системи початкового рівня компанії Sun створюють основу для вирішення обчислювальної обробки даних в масштабі підприємства, на базі сіткової моделі обчислення, яка використовується в таких областях, як статистика, графічний і структурний аналіз, молекулярна і обчислювальна хімія. Лінійка серверів Sun Grid Rack System представлена серверами Sun Fire V20z або V40z, які побудовані на основі процесора Opteron [59].

Сіткові обчислення пропонують можливість перенести обчислювальне навантаження на численні системи і в той же час забезпечують можливість виконання менш важких завдань на окремому комп'ютері в “сітці”. Не слід думати про сіткову систему, такий як Grid Rack System компанії Sun, як про кластер або розподілену систему. Уявимо собі мережеві обчислення як спосіб виконання проектів по обробці даних з масовим паралелізмом. Щоб зробити можливими сіткові обчислення, системи оснащують інструментами управління і програмним забезпеченням, яке керує розподілом навантаження серед систем, які є частиною “мережі”. Очікується, що мережеві обчислення можуть стати частиною широкомасштабних обчислювальних технологій, де обробка даних буде доступна в будь-якому місці “мережі”.

2.2.2 Сервери середнього рівня

З точки зору компанії Sun, сервер середнього рівня – це потужна система, яка пропонує поліпшені робочі характеристики за розумною ціною. Систему середнього рівня відрізняє від системи початкового рівня той факт, що сервер середнього рівня пропонує підвищену міру відмовостійкості, а також високу доступність. Системи середнього рівня також оснащені засобами, що забезпечують підтримку більшої кількості інструментів управління. В таблиці 2.3 представлені основні моделі, що представляють лінійку серверів середнього рівня компанії Sun [59].

Таблиця 2.3 – Сервери середнього рівня компанії Sun

Модель	Центральний процесор	Тактова частота, ГГц	Роз'єми вводу-виводу даних	Максимальна підтримувана пам'ять Гбайт	Домени	Максимальний об'єм зовнішньої пам'яті	Ресурсоємність
Sun Fire V480	До 4 процесорів UltraSPARC III 1.2	6 PCI	32	1	Немає даних	SC	
Sun Fire V490	До 4 процесорів UltraSPARC IV	1,05/1,35	6 PCI	32	1	Немає даних	SC
Sun Fire V880	До 8 процесорів UltraSPARC III	1,2	9 PCI	64	1	Немає даних	SC
Sun Fire V890	До 8 процесорів UltraSPARC IV	1,2/1,35	9 PCI	64	1	Немає даних	SC
Sun Fire V1280	До 12 процесорів UltraSPARC III	1,2	6 PCI	96	1	Немає даних	SC
Sun Fire E2900	До 12 процесорів UltraSPARC IV	1,05/1,2/1,35	6 PCI	96	1	17 Тбайт	SC
Sun Fire 4800	До 4 процесорів UltraSPARC III	1,05/1,2	16 PCI або 8 PCI+	96	1-2	35 Тбайт	DSD, SC
Sun Fire E4900	До 12 процесорів UltraSPARC IV	1,05/1,2/1.35	16PCI+	96	1-2	36 Тбайт	DSD, SC
Sun Fire 6800	До 24 процесорів UltraSPARC III	1,05/1,2	32 PCI/.16 PCI+	192	1-4	Немає даних	DSD, SC
Sun Fire E6900	До 24 процесорів UltraSPARC IV	1,05/1,2/1,35	32 PCI+	192	1-4	77 Тбайт	DSD, SC

2.2.3 Високопродуктивні сервери

Високопродуктивні сервери компанії Sun позиціонуються як заміна мейнфреймів. Ці сервери можуть підтримувати від 36 до 72 процесорів

UltraSPARC. Вони пропонуються на ринку в якості вкрай відмовостійких, критично важливих серверів, призначених для центрів обробки даних. Високопродуктивні сервери компанії Sun призначені для роботи без простою, вони поставляються з набором характеристик, які дозволяють змінювати їх конфігурацію під час експлуатації.

Таблиця 2.4 – Високопродуктивні сервери компанії Sun

Модель	Центральний процесор	Тактова частота, ГГц	Роз'єми вводу-виводу	Максимальна пам'ять, Гбайт	Домени	Максимальний об'єм зовнішньої пам'яті	Споживання
Sun Fire 12K	До 52 процесорів UltraSPARC III	1,05/1,2	36 PCI	288	1-9	120 Тбайт	DSD, SC
Sun Fire 15K	До 106 процесорів UltraSPARC III	1,05/1,35	72 PCI	576	1-18	250 Тбайт	DSD, SC
Sun Fire E20K	До 36 процесорів UltraSPARC IV	1,05/1,2	36 PCI+	288	1-9	120+ Тбайт	DSD, SC
Sun Fire E25K	До 82 процесорів UltraSPARC IV	1,05/1,2/1,35	72 PCI+	576	1-18	250+ Тбайт	DSD, SC

Високо-продуктивні сервери компанії Sun поставляються з деталями, що допускають заміну під час роботи, і шинною структурою. Властивість динамічної реконфігурації (Dynamic Reconfiguration - DR), яка властиво Solaris 8, дозволяє реконфігурувати компонент ядра в той час, коли продовжують виконуватися Solaris і застосування. За допомогою динамічної реконфігурації

можна в "гарячому" режимі замінювати мікросхеми пам'яті, PCI-карти, центральні процесори і інші компоненти. Окрім властивості динамічної реконфігурації, високопродуктивним серверам властиво така властивість, як домен динамічної системи (dynamic system domains), яке дозволяє запускати копії операційної системи Solaris і застосування на одному і тому ж сервері [60].

В таблиці 2.4 приведено чотири поточні компоненти лінійки високопродуктивних серверів компанії Sun.

Компанія Sun також пропонує лінійку комп'ютерів SPARC64-V корпоративного класу Fujitsu PRIMEPOWER. У цій лінійці представлено сім систем: PRIMEPOWER 250-2500.

2.2.4 Блейд-сервери

Стратегія компанії Sun, що передбачає виробництво і підтримку блейд-серверів, була важливою частиною маркетингу архітектури масштабованого сервера компанії аж до червня 2005 року. Саме цього року компанія Sun зняла з виробництва свою лінійку блейд-серверів, включаючи корпусну систему Sun Fire B1600, Sun Fire B100s, Sun Fire Bl00x, Sun Fire B200, Sun Fire B10n Content Load Balancing Bridge, Sun Fire Bl0p SSL Proxy Blade і Sun N1 Blades Starter Pack. [61]

– Блейд-сервери, які працюватимуть на основі процесорів AMD x86 Opteron і операційної системи Linux.

– Блейд-сервери, які працюватимуть на основі процесора UltraSPARC і операційної системи Solaris.

Важливість блейд-серверів для компанії Sun і інших виробників апаратного забезпечення пояснюється можливістю за їх допомогою виконувати горизонтальне масштабування системи. Сервери цієї категорії грають важливу роль на деяких ключових ринках компанії Sun - відмовостійкі кластери, Інтернет, телекомунікації і так далі. Деякі застосування рівня підприємства, які

виконуються на серверах компанії Sun, перепроектуються для роботи на блейд-серверах. Це також відноситься до IBM DB2 і Oracle.

У конфігурації блейд-серверів комп'ютерна системна плата перероблена таким чином, що вона стає компонентом типу "подключи і працюй", замінюваною в "гарячому" режимі прямо в корпусі блейд-сервера. Цей корпус регулює енергопостачання і повітряне охолодження для встановлених блейд-серверів. За допомогою блейд-серверів центр обробки даних може відмовитися від масивних стійок обробки даних, таких, що містять близько 200 серверів, розміром з домашній холодильник.

Насущна проблема, що стосується блейд-серверів, полягає в тому, що ці системи все ще не повністю стандартизовані. Серед виробників серверів існує конкуренція з продажу кластерних серверів, але ринок все ще відносно молодий. З цієї причини, повний набір характеристик блейд-сервера відрізняється для різних постачальників OEM [61].

2.2.5 Сервери зберігання даних

Компанія Sun – один з найважливіших гравців на ринку сховищ даних, реалізованих на апаратному рівні, особливо у вигляді серверних платформ. Пропонується безліч пристроїв зберігання даних – від маленьких пристроїв до дискових масивів корпоративного класу з мікропроцесорним управлінням, а також супутнє програмне забезпечення. Але найбільше значення в індустрії сховищ даних має стратегічна серверна платформа, пропонована Sun. У центрах обробки даних застосовуються дві керуючі серверні платформи: сервери Microsoft Windows і сервери Sun Solaris. Практично будь-яке застосування сховища даних або сервер-сховище даних великого підприємства, яке претендує на багатоплатформність або різнорідність, підтримує ці дві серверні платформи. Велика частина найбільш важливого програмного забезпечення сервера-сховища даних починала свій шлях з Sun Solaris, а потім був здійснений перехід на інші операційні системи. [62]

Компанія Sun розширила спектр пропозицій сховищ даних, створюючи і перетворюючи свої сервери в платформи-сховища даних. Вона також придбала ряд компаній, які мають вплив на ринку сховищ даних, включаючи HighGround, у зв'язку з її програмним забезпеченням управління ресурсами зберігання даних; Cobalt – у зв'язку з її пристроями, а літом 2005 року StorageTek – одного з виробників апаратного забезпечення, які реалізують технологію зберігання даних на корпоративному рівні.

В додатку Б приводиться перелік апаратних засобів, які використовуються для створення сховищ даних Sun.

Сервери зберігання даних (або, як їх ще називають, сервери-сховища даних) StorEdge компанії Sun популярні у покупців серверів Sun, але не такі популярні в організацій, що вкладають великі кошти в EMC, Hewlett-Packard або в сховища пам'яті інших виробників. Вони також не такі популярні в організацій, що орієнтуються на рішення сховищ даних відкритого типу. Як показано в додатку Б, компанія Sun пропонує безліч систем з торговою маркою StorEdge, включаючи певну кількість систем, створених іншими виробниками, а потім випускаються під маркою Sun. Це звичайна практика в технології зберігання даних.

Певна кількість застосувань управління даними представлені в комплексі з серверами зберігання даних компанії Sun. Нижче наведено перелік відповідних програм.

– *Sun Java StorEdge.* До складу цього пакету входять програми Consolidation Suite, Continuity Suite, Content Suite і Compliance Suite.

– *Управління даними.* Цей пакет включає програми StorEdge QFS, StorEdge SAM-FS, а також необов'язкові програми VERITAS Storage Foundation, File System і Volume Management.

– *Захист даних.* У цей пакет включені StorEdge Availability Suite, StorEdge Enterprise Backup, StorEdge Data Snapshot, StorEdge Data Mirror, StorEdge Data Replication і StorEdge Archiving, а також додаткові програми VERITAS NetBackup і NetBackup Enterprise Server.

– *Управління сховищами даних.* Цей пакет включає програми StorEdge Enterprise Storage Manager, StorEdge Traffic Manager, Storage Automatic Diagnostic Environment і StorEdge Pool Manager Software [62].

2.2.6 Кластери Sun

Інтегрована апаратно-програмна платформа Sun Cluster може застосовуватися для створення кластера, що об'єднує до 16 вузлів серверів Sun, реалізованих на платформах SPARC або x86. Остання версія ПЗ цього типу під назвою Sun Cluster 3.1 виконується у вигляді надбудови над ОС Solaris і поширюється у вигляді комплексного рішення, яке включає міжмережеві технології, зовнішнє сховище і служби Sun. Пакет Cluster 3.1 використовує ПЗ Solaris IP Multipathing (iPMP), яке забезпечує підтримку для багатомережевих серверів, а також декількох мережевих інтерфейсів. Все це дозволяє поліпшити продуктивність підсистеми вводу-виводу даних і усієї системи в цілому.

Пакет Sun Cluster 3 підтримує динамічну реконфігурацію кластерного обладнання, включаючи встановлення або видалення центральних процесорів, пам'яті, плат вводу-виводу і інших пристроїв. Таким чином, існує можливість демонтувати процесорні плати сервера Sun, замінити їх більш швидкодіючими блоками, не розбираючи при цьому сам сервер або кластер. Компанія Sun називає цю технологію динамічною реконфігурацією в режимі реального часу. Програма динамічної реконфігурації "вступає в гру" у разі виявлення проблеми з установкою або видаленням пристроїв.

Кластери компанії Sun можуть включати 16 вузлових серверів, що робить можливим створення застосувань класу "мейнфрейм" на основі Sun Cluster 3.1. На цій платформі були створені деякі дуже великі бази даних, включаючи Oracle9i RAC (real application cluster).

Застосування управління кластерами компанії Sun називається SunPlex Manager. При його використанні кластер керується як окрема система. Утиліта управління з графічним інтерфейсом, що входить до складу Sun Management Center, є модуль Sun Cluster, який може виявляти стан елементів кластера Sun

за допомогою пасток SNMP. При цьому застосовується набір агентів SNMP. Нижче представлені агенти і утиліти SNMP незалежних постачальників, яких можна використовувати для відстежування і керування кластером Sun.

Сервери компанії Sun комплектуються набором застосувань, створюючи платформу, названу Sun java Enterprise System, до складу якої входять наступні компоненти [60]:

– веб-сервери/веб-служби;

– сервери застосувань, включаючи календарні застосування;

– служба установки ідентичності мережі (network identity - то, що компанія Sun називає службою доступу і аутентифікації);

– служби зв'язку, обміну повідомленнями і виробничої співпраці;

– компонент, призначений для створення порталу (веб-інтерфейс, призначений для численних служб);

– служби безпеки;

– служби каталогів;

– служби забезпечення доступності.

Рішення Java Enterprise System може застосовуватися для некластеризованих версій серверів Sun, але при створенні цих застосувань для кластера їх можна масштабувати, надаючи велику відмовостійкість. Прикладом реалізації на практиці є Sun Enterprise Continuity Solution – система віддаленого підключення, реалізована на основі Sun Cluster 3.1. При цьому забезпечується розміщення вузлів кластера Sun Cluster на відстань до 200 км. Як тільки вузол кластера в центрі обробки даних відключається, оперативно підключається віддалений вузол.

Крім того, компанія Sun підтримує веб-службу Sun Cluster Global Network Service, яка дозволяє створювати надбудову над кластером Sun, а також вирівнювати навантаження застосування і його доступності. Використання Sun Cluster Global Network Service означає, що навіть якщо вузли кластера географічно розділені, не варто встановлювати службу розподілу

навантаження і наділяти її відмовостійкістю, оскільки служба Sun доступна через Інтернет. Інші консолідовані служби включають Global Network Service, Global Devices і Global File Services. Функціонування усіх служб під назвою "global" означає спільне управління мережевими ресурсами за допомогою керуючого програмного забезпечення кластера. Також можна використовувати файлову систему UFS або VERITAS VxFS в якості файлової системи кластера замість Global File Service [60].

Технологія Sun Custer 3 має деякі унікальні характеристики. Кластер Sun може каталогізувати пам'ять і за допомогою віддаленої загальної пам'яті (RSM) забезпечує використання застосуванням технології швидкого міжкомпонентного з'єднання для прямого звертання до пам'яті в кластері, навіть якщо вузли кластера недоступні. Віддалена загальна пам'ять (RSM) використовує технологію Scalable Coherent Interconnect (SCI - PCI) для обходу передачі даних через Ethernet. Завдяки віддаленій загальній пам'яті полегшується створення високоефективних застосувань баз даних. Ще одна властивість, Application Traffic Striping, дозволяє розподіляти IP-трафік по численних міжкомпонентних з'єднаннях.

2.2.7 NEBS-сертифіковані сервери

Телекомунікаційний стандарт Telcordia (раніше Belcore) Network Equipment – Building System (NEBS) визначає, яке устаткування може використовуватися в телекомунікаційній мережі як частина ILEC або центрального офісу компанії Regional Bell Operating Company (RBOC). Стандарт був прийнятий в 1970-х роках і використовується виробниками серверів як орієнтир, що допомагає реалізувати продукцію на цьому вкрай насиченому ринку. Цього стандарту дотримуються компанії Verizon, Qwest, SBC і AT&T. Прикладом його реалізації служить ПЗ Telcordia, використовуване як в дротових, так і бездротових мережах. Сертифікація на предмет відповідності цьому стандарту припускає представлення зразка серверної продукції компанії в агентство по сертифікації.

Компанія Sun виробляє лінійку серверів, яку використовують провайдери мережевого устаткування для своїх центральних офісів. Тут представлене найрізноманітніше обладнання - від кластерних серверів 1U до сервера 12U Netra 1280. Рекомендуються до застосування: сервери застосувань, контрольні точки, шлюзи, регістри місцезнаходження, платформи мережевого керування, сервери передачі мультимедійних потоків, комутація, голосова телефонія і VoIP (телефонія на базі IP), веб- і кеш-сервери.

2.3 Висновки до другого розділу

В другому розділі проведено аналіз серверів Sun Microsystems.

Проаналізовано конфігурацію і технічні параметри серверів і процесорів SPARC, а зокрема архітектуру RISC і процесори SPARC і UltraSPARC. Проведено аналіз категорії серверів: сервери початкового рівня, сервери середнього рівня, високопродуктивні сервери, блейд-сервери, сервери зберігання даних, кластери Sun та NEBS-сертифіковані сервери.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Аналіз завдання

Для того, щоб провести оптимізацію роботи мережевої системи підприємства, проаналізуємо її.

На рисунку 3.1 представлено організаційно-штатну структуру підрозділу. На чолі підрозділу стоїть начальник підрозділу. До складу підрозділу входять 3 відділення, а також спеціалізований відділ прямого підпорядкування начальнику. Кожне відділення поділяється на 2 підвідділи. Кожен підвідділ, у свою чергу, розділяється на 3 сектори.

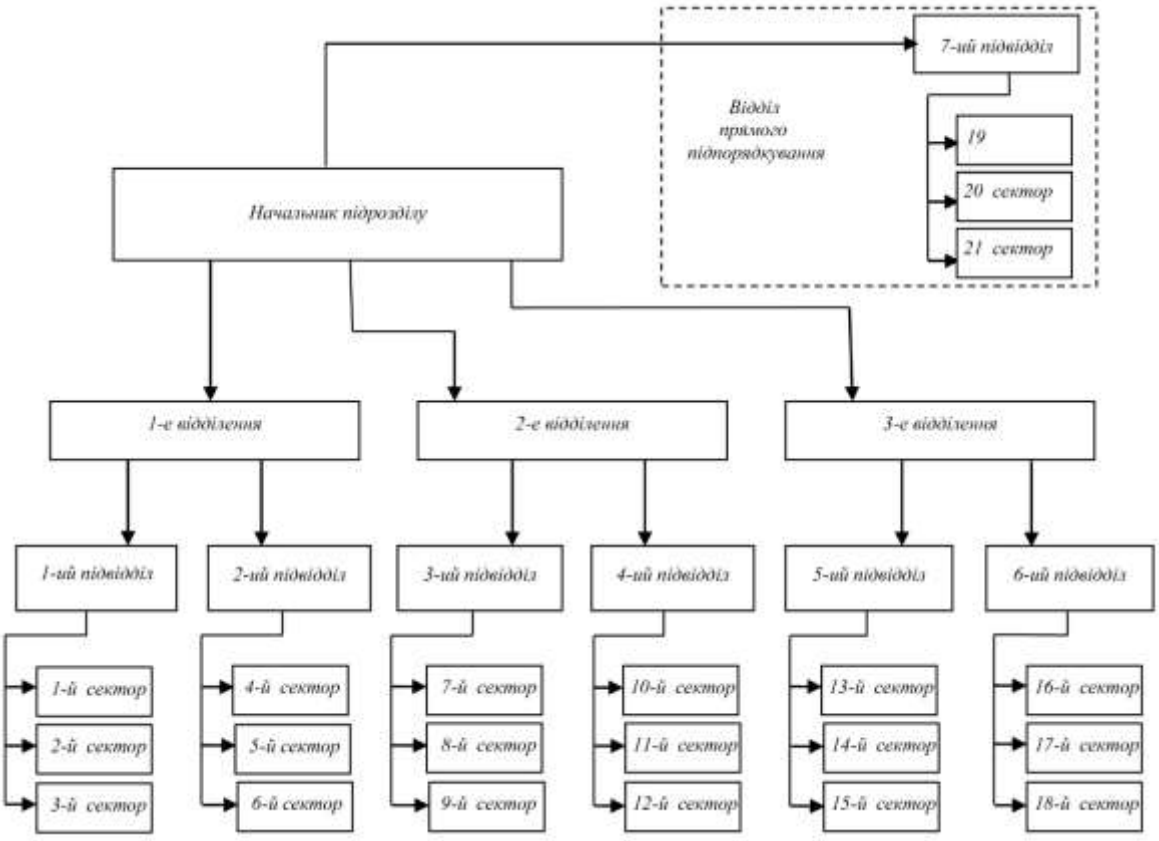

Рисунок 3.1 – Організаційна структура підрозділу

Усього в підрозділі задіяно 60 чоловік, яким передбачається виділити в користування персональний комп'ютер.

Враховуючи те, що в якості захисту використовується тільки антивірусне програмне забезпечення, то наразі дане використання СЗІ є неповним.

В даному розділі розробимо методику забезпечення захисту мережевої системи.

3.3 Використання системи захисту конфіденційної інформації PGP

На робочі станції мережевої системи буде встановлено та застосовано СЗКІ PGP.

3.3.1 Основні характеристики системи PGP

PGP об'єднує в собі кращі сторони симетричної криптографії і криптографії з відкритим ключем. PGP – це гібридна криптосистема. Засіб захисту вбудовується в оболонку операційної системи, надає користувачеві можливість зашифровувати файли на вимогу через контекстне меню провідника або спеціальних клавіш.

При шифруванні файлів або поштових повідомлень PGP створює одноразовий симетричний ключ, який використовується для єдиного сеансу зв'язку. Сеансовий ключ є псевдовипадковим числом, згенерованим від випадкових рухів мишки і натиснень клавіш. Сеансовий ключ використовується надійним і швидким симетричним алгоритмом, яким PGP зашифровує повідомлення, перетворюючи його на шифротекст. Для підвищення криптостійкості, зниження навантаження на канали зв'язку і економії дискового простору в системі застосовується стискання інформації. Сеансовий ключ зашифровується відкритим ключем одержувача. Зашифрований відкритим ключем одержувача сеансовий ключ "прикріпляється" до шифротексту і передається разом з ним отримувачу, утворюючи так званий "цифровий конверт" зображено на рисунку 3.2.

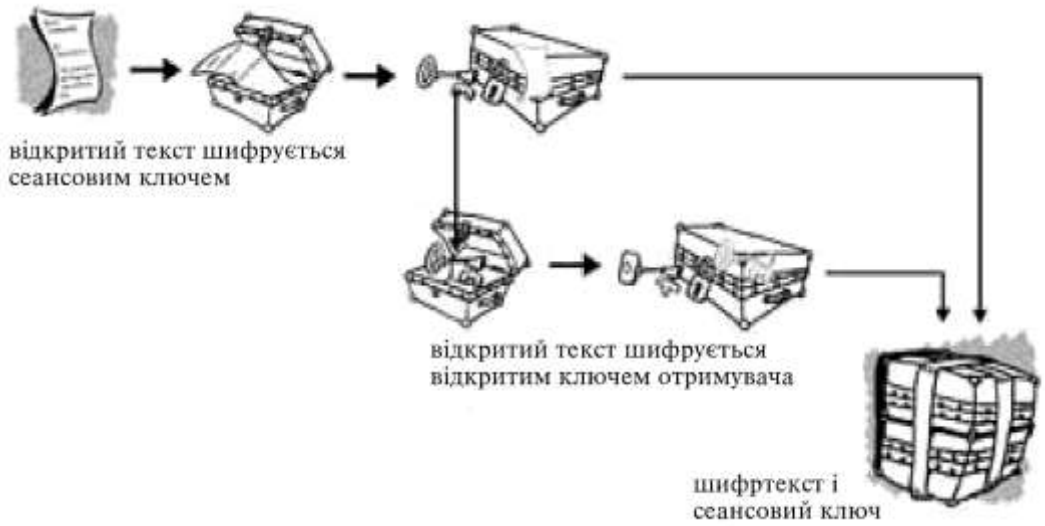

Рисунок 3.2 – Формування цифрового конверта

Розшифрування цифрового конверта відбувається в зворотному порядку. На приймальній стороні система PGP використовує закритий ключ одержувача для отримання з повідомлення сеансового ключа. Отриманий сеансовий ключ PGP, використовує для перетворення початкового повідомлення у відкритий текст [63].

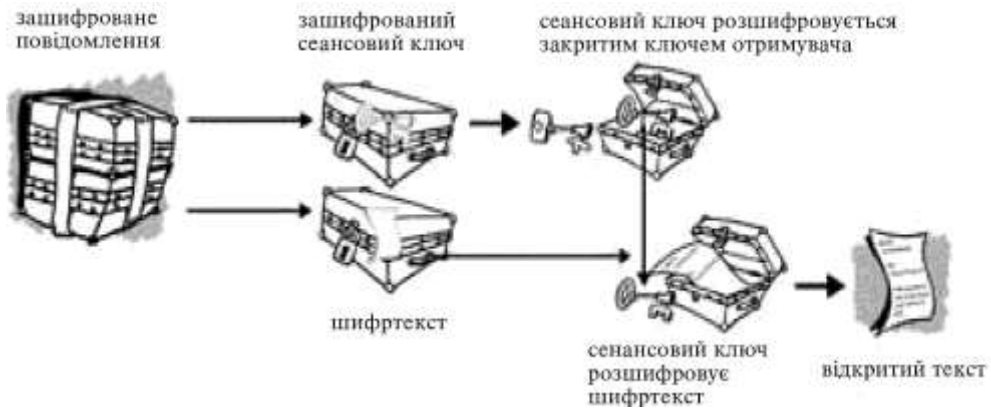

Рисунок 3.3 – Розшифровка цифрового конверта

Використовувані спільно системи шифрування взаємно доповнюють один одного без будь-якого збитку безпеки. Симетричне шифрування, швидкість і надійність якого в тисячі разів швидше асиметричного, забезпечує висока швидкодія і криптостійкість системи. Можливість розподілу ключів по відкритих каналах зв'язку, що надається схемою шифрування відкритим ключем, у свою чергу, надає просте рішення проблеми розподілу ключів.

3.3.2 Ініціалізація системи PGP на робочій станції

Установка системи PGP на робочу станцію надзвичайно проста. Для ініціалізації системи PGP необхідно закрити всі працюючі застосування Windows і запустити файл PGPDesktop.exe, який відкриє вікно діалогової установки цієї програми. Окрім стандартних ліцензійних угод при її ініціалізації слід дотримувати декілька правил [63].

У вікні "User type" (зображено на рисунку 3.4) необхідно вибрати опцію "No, I'm a New User", з тим, щоб при встановленні системи користувачеві ініціалізувалася пара (відкритий і закритий) ключів. Якщо вибрати пункт "Yes, I already have keyrings", то ініціалізувати ключі можна буде пізніше, користуючись менеджером ключів.

Основні виконувані програмні блоки PGP встановлюються в директорію. Якщо немає приписів системного адміністратора, то слід прийняти пропозицію програми-мага системи. У вікні вибору компонентів "Select Component" визначається набір функцій, встановлюваний на робочу станцію. На рисунку 3.5 приведений набір компонентів, пропонований системою.

При ініціалізації системи в режимі "No, I'm a New User" здійснюється генерація пари симетричних ключів для нового користувача. По замовчуванню система PGP встановлює розмір персональних ключів користувача, рівний 2048 біт, алгоритм несиметричного шифрування – RSA і термін дії сигнатур (ключів) – один рік. Індивідуальні параметри шифрування можна встановити, якщо у вікні "Key Generation Wizard" натиснути кнопку "Expert" (рис. 3.6). При цьому

відкриється вікно вибору параметрів шифрування "Expert Key Parameter Selection" (рис. 3.7), в якому треба ввести повне ім'я користувача, поштова адреса і вибрати необхідні параметри ключів і алгоритм шифрування. Якщо інформація про користувача не буде введена у вікні "Expert Key Parameter Selection", то система запропонує її ввести в спеціальному вікні "Name and E - mail Assignment" [63].

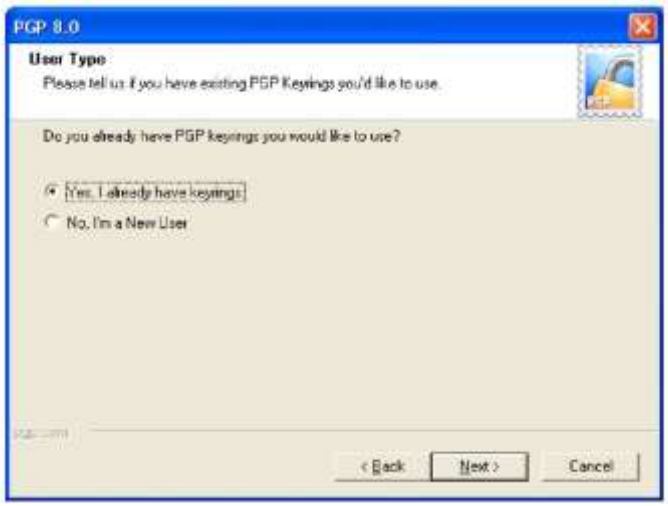

Рисунок 3.4 – Вибір "типу" користувача

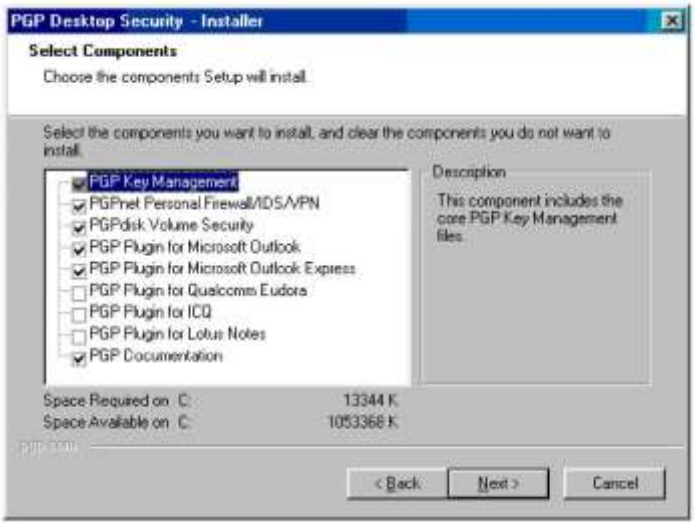

Рисунок 3.5 – Меню вибору встановлюваних компонентів системи

Рисунок 3.6 – Вікно майстра генерації ключів

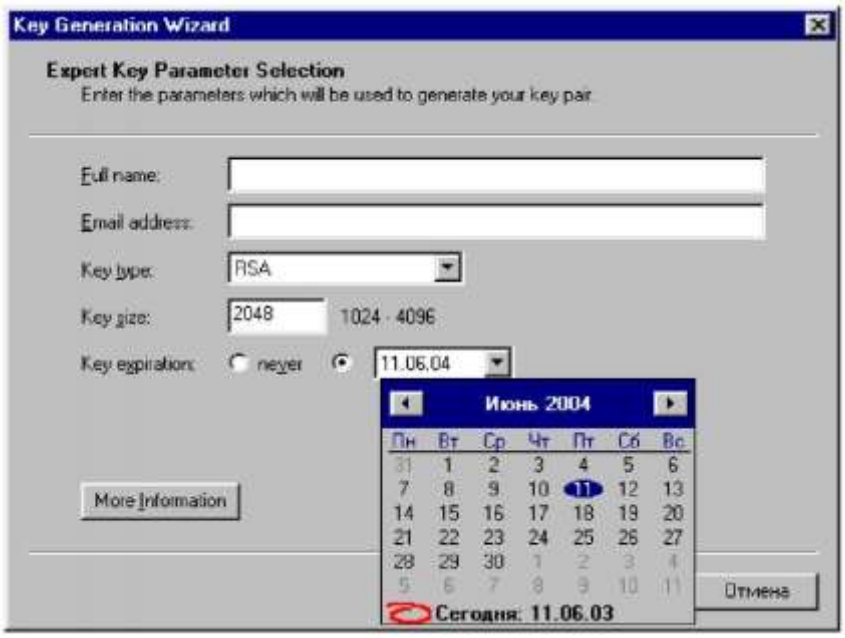

Рисунок 3.7 – Вибір параметрів ключів і алгоритму шифрування

В наступному вікні "Passphrase Assignment" задається (і підтверджується) пароль користувача (рис. 3.8), на основі якого генерується секретний і відкритий ключі. PGP не обмежує знизу кількість символів в паролі, але рекомендує, щоб їх було не менше вісім. У вікні "Passphrase

Assignment" індукується якість "Passphrase Quality" ключової фрази, що вводиться. Після підтвердження введення пароля здійснюється покрокова генерація пари ключів (Key Generation і Generation Subkey), що супроводжується відповідною індикацією у вікні "Key Generation Progress". Для завершення ініціалізації PGP на робочу станцію необхідно перенавантажувати комп'ютер, встановивши перемикач "Yes, I want to restart my computer now" у включений стан [63].

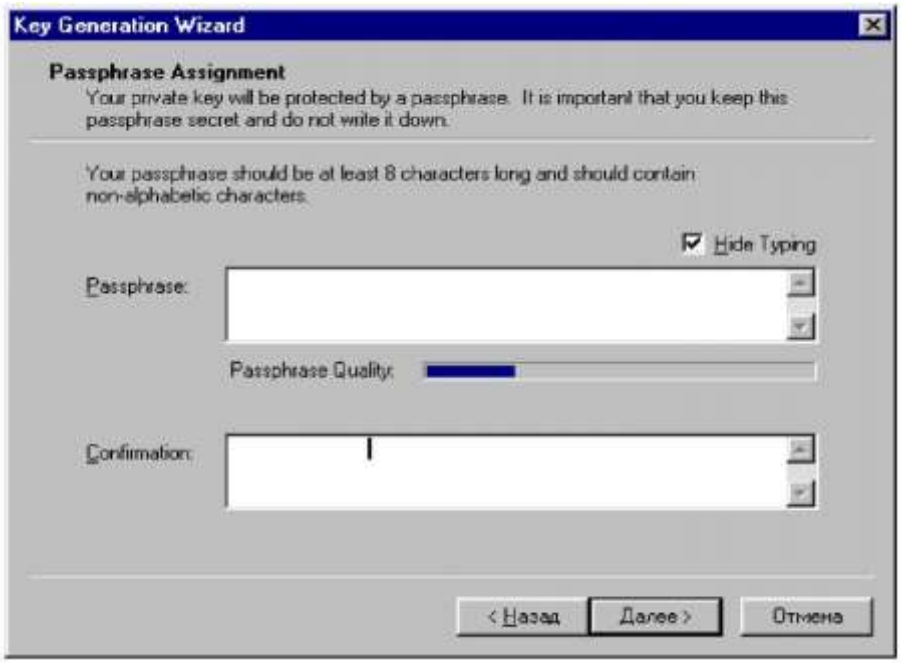

Рисунок 3.8 – Введення ключової фрази

При необхідності ввести в систему нового користувача або змінити параметри шифрування існуючого вікно "Key Generation Wizard" може бути викликане з меню встановленої програми PGP → PGPkeys → Keys → New Key…

Процес ініціалізації POP закінчується перезапуском операційної системи. Після установки в меню “пуск” → “все программы”, створюється нова група PGP, в якій знаходяться ярлики програм, що входять до складу системи: “PGPdisk”, “PGPkeys” і “PGPmail”. “PGPdisk” служить для створення і роботи із захищеними логічними дисками; “PGPkeys” – для створення, редагування,

отримання і управління ключами; “PGPmail” – для обробки шифрування і дешифрування файлів [63].

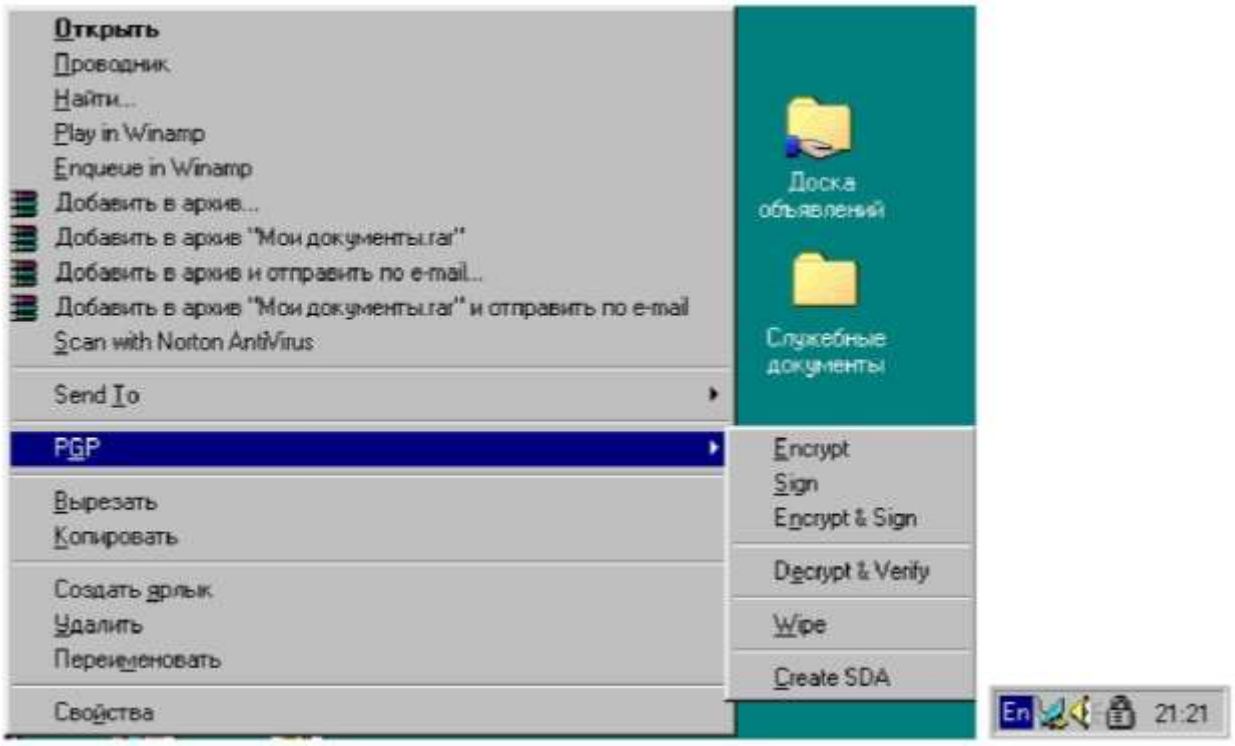

Рисунок 3.9 – Ознаки успішної ініціалізації PGP на робочій станції

Успішна ініціалізація системи PGP супроводжується появою на панелі завдань значка у вигляді навісного замка, рядки PGP в меню Пуск → Программы → PGP і рядки в спливаючому меню, що з'являється при натисненні правої клавіші миші на ярлику документу або каталогу з документами (рис. 3.9).

3.3.3 Генерація, імпортування і експортування ключів

Користувачі ПК можуть мати декілька пар ключів для обміну приватними даними з різними категоріями учасників документообігу. На режимних підприємствах часто доступ в глобальні мережі має один комп’ютер, за допомогою якого співробітники підприємства отримують і відправляють пошту. Тому на одному комп'ютері в системі PGP одночасно може бути зареєстровано декілька користувачів з унікальними іменами і ключами. Для

генерації нового ключа (новому користувачеві) необхідно викликати головне меню PGP, натиснувши кнопку системи PGP на панелі завдань, і вибрати вікно "PGPkeys", в якому здійснюються основні маніпуляції з ключами (рис. 3.10). В меню вікна "PGPkeys" викликати підменю "Keys" і натиснути кнопку “New Key”: PGP → PGPkeys → Keys → New Key. Після чого з'явиться діалогове вікно "Key Generation Wizard", яке з'являлось при ініціалізації системи PGP на комп’ютер. Ініційовані ключі знову зареєстрованого користувача відображуються у вигляді відповідного рядка у вікні "PGPkeys" з ім'ям користувача [63].

Рисунок 3.10 – Вікно "PGPkeys"

Всі ключі зберігаються по замовчуванню в папці “C:\Documents and Settings\%Userprofiles%\Мои документы\PGP”. Але за бажання її можна змінити, для чого достатньо натиснути комбінацію клавіш “Ctrl-T” або вибрати меню “Edit-Options” і в закладці "files" вписати бажаний шлях і імена файлів для зберігання ключів. Якщо до цього моменту в системі вже були створені ключі, то програма запропонує скопіювати зміст файлу з ключами в нову директорію.

Для організації шифрованого зв'язку учасникам обміну, що працюють на різних ПК локальної (глобальною) мережі, необхідно обмінятися відкритими ключами. Найбільш зручним способом обміну ключами є їх пересилка через

сервер-депозитарій або за допомогою поштових сервісів. Інколи може потрібно відправити відкритий ключ у вигляді окремого файлу (наприклад, через FTP-сервер). В цьому випадку можна експортувати або копіювати ключі у файл. Щоб зберегти ключ у вигляді окремого файлу необхідно у вікні "PGPkeys" виділити ключ, що підлягає експортуванню, в рядку меню натиснути кнопку “Keys → Export” і вказати ім'я файлу і каталог призначення. При цьому допускається експортування групи ключів, шляхом виділення декількох потрібних. Отриманий файл з відкритим ключем може бути переданий по мережі або на будь-якому іншому носієві.

Асиметричні криптосистеми вирішують проблему обміну ключами і зашифрованою інформацією, проте вони вкрай вразливі до атак "людина в середині", коли зловмисник намагається видати свої підробні відкриті ключі за ключі кореспондентів, що беруть участь в двосторонньому обміні. Пізніше це дозволить йому повністю контролювати повідомлення, що пересилаються: перехоплювати, читати і змінювати. Взаємне завірення користувачами відкритих ключів один одного безпосередньо після обміну – це основа розподіленої моделі довіри "Web of Trust" системи PGP, що забезпечує протидію таким атакам. Для того, щоб переконатися в легальності знову імпортованого ключа в системі є можливість порівнювати сигнатури відкритого ключа на комп'ютері-одержувачі і комп'ютері-джерелі. Користувач, що переслав свій відкритий ключ і користувач, що отримав його, повинні одночасно відкрити підменю "Keys" вікон "PGPkeys" і передивитися властивості "Properties" ключа, що перевіряється, і порівняти їх сигнатури (рис. 3.11). Переконавшись в істинності ключа, одержувач може "підписати" його.

Щоб підписати відкритий ключ або будь-які з відомостей його сертифікату потрібно у вікні "PGPkeys" виділити ключ або будь-які з відомостей сертифікату, що підлягають завіренню підписом, в рядку меню вибрати команду "Sign" підменю "Keys" і ввести свій пароль. Легітимні ключі, яким тепер довіряє користувач цієї системи PGP, забарвлюються у вікні "PGPkeys" в зелений колір [59].

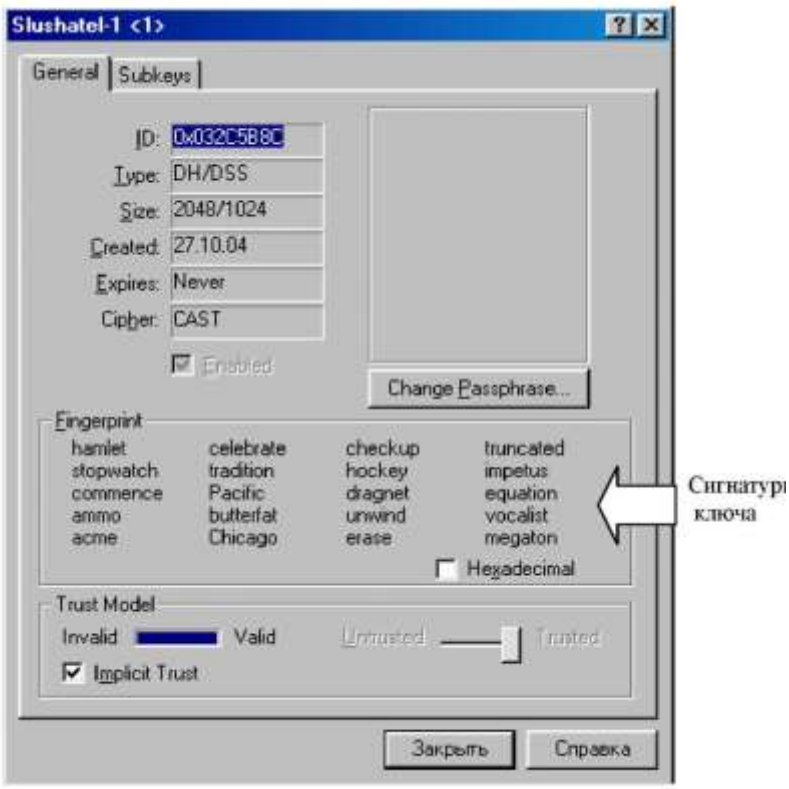

Рисунок 3.11 – Перевірка легітимності отриманого ключа

В системі є можливість підписувати ключову інформацію партнерів особливим чином. Для цього необхідно натиснути кнопку "Sign the selected item в панелі інструментів", у вікні, що з'явилося, проглянути список підписуваних ключів, відомостей сертифікату і їх відбитків і переконатися, що не вибрано нічого зайвого, натиснути кнопку "More Choices" і в розділі "Signature Type" слід вказати тип підписи, яким хочете завірити ключ, запис сертифікату:

– Non-exportable – підпис, що не експортується, – коли користувач впевнений в достовірності ключа або запису сертифікату, але не хоче виступати його поручителем. Такий підпис не може бути експортований і служить тільки для інформування програми в тому, що користувач вважає ключ не скомпрометованим, і дозволяє наділити власника певним рівнем довіри в завіренні інших ключів.

– Exportable – підпис, що експортується, – коли користувач впевнений в справжності ключа або запису сертифікату і хоче виступати його поручителем. Такий підпис експортується разом з ключем, щоб інші

користувачі могли на неї покладатися при визначенні достовірності цього ключа.

– Trusted Introducer Exportable – використовується, коли користувач впевнений в достовірності ключа партнера і готовий наділити його повноваженнями довіренного поручительства: всі завірені довіреним партнером ключі стають апріорі достовірними як для самого користувача, так і для всіх, хто довіряє його підписи.

– Meta-Introducer Non-Exportable – завірення таким підписом якого-небудь ключа зробить його власника мета-поручителем користувача комп'ютера: власники всіх підписаних власником імпортованого ключа стають довіреними поручителями користувача (тобто будуть, як би завірені підписами Trusted Introducer Exportable). Цей підпис не експортується.

При виборі одного з двох останніх типів підпису, надаються додаткові нагоди:

– Maximum Trust Depth – на скільки рівнів вниз уздовж ланцюга сертифікації відбуватиметься завірення ключів довіреним поручителем або наділення повноваженнями довіреного поручительства від мета-поручителя.

– Domain restriction – обмеження для довіреного поручителя на завірення ключів, що належать тільки до вказаного домена. Наприклад, якщо вказати pgpua.com, довірений поручитель зможе завіряти лише ті ключі, чиї email-адреси закінчуються на pgpua.com.

Кращий спосіб встановити достовірність отриманої копії відкритого ключа кореспондента – подзвонити йому і попросити прочитати відбиток з оригіналу, що зберігається на його зв'язці (прочитати відбиток повинен саме відправник одержувачеві, а не навпаки!). Малоймовірно, що зловмисник зможе перехопити такий довільний дзвінок і провести активну атаку, спробувавши видати себе за кореспондента. Якщо кореспондентові - одержувачеві знайомий голос кореспондента - відправника, це зробити буде практично неможливо [60].

3.3.4 Шифрування і обмін шифрованою інформацією

Незашифрована особиста інформація (редаговані текстові файли, малюнки, таблиці і так далі), розшифровані файли, отримані від інших членів обміну, не мають бути доступні користувачам по мережі. Тому вони повинні оброблятися (редагуватися, зашифровуватися і розшифровуватися) в каталозі, до якого немає мережевого доступу. При обміні конфіденційною інформацією в системі реалізується режим шифрування за вимогою. Призначений для відправлення по відкритих каналах зв'язку документ має бути відредагований у відповідному формату документу стандартному застосуванні і закритий. Цей документ не піддавався ще криптографічному перетворенню і містить приватні відомості у відкритому виді. Для шифрування документу за допомогою системи PGP необхідно підвести курсор миші до його ярлика і натиснути праву клавішу маніпулятора. У вспливаючому меню слід вибрати один з трьох варіантів шифрування файлу (рис. 3.12):

- Encrypt – зашифрувати файл (документ);
- Sign – сформувати під документом електронний цифровий підпис;
- Encrypt & sign – зашифрувати і підписати документ.

В першому випадку в поточній папці формується файл, що містить інформацію в зашифрованому виді. В другому випадку, в поточній папці формується файл, що містить електронний цифровий підпис (ЕЦП) власника початкового документу. В третьому випадку – єдиний файл, одночасно містить інформацію в зашифрованому виді і ЕЦП.

При виборі пунктів “Encrypt” або “Encrypt & Sign” з’являється вікно вибору ключа (PGP Key Selection). У вікні з верхньої половини екрану слід вибирати реципієнта (одержувача), чиїм ключем ми шифруватимемо, клацаємо подвійним натисненням миші по ньому і він автоматично переноситься вниз.У лівому нижньому кутку цього вікна є 4 опції для шифрування. Можна варіювати цими опціями залежно від даних, які потрібно зашифрувати:

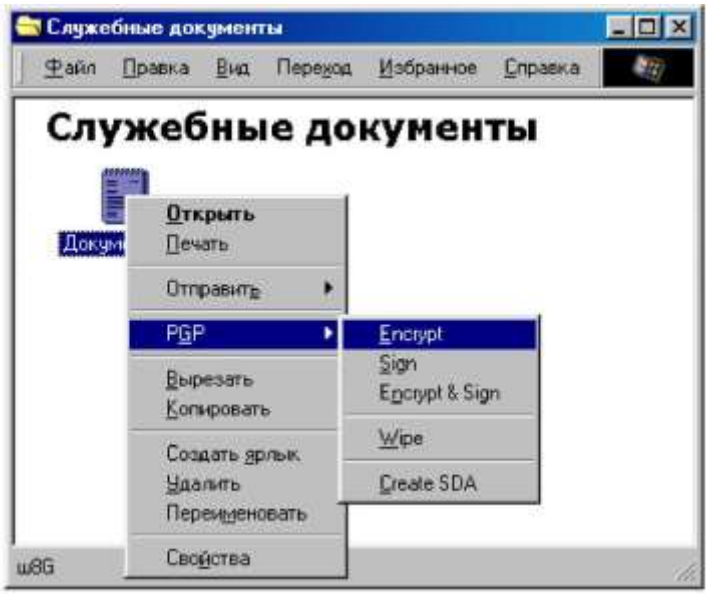

Рисунок 3.12 – Вибір режиму зашифрования документу

Рисунок 3.13 – Вибір відправника і одержувача зашифрованого документу

– Text Output (“текст на виході”). Коли користувач відправляє файли поштою, прикріплюючи їх до листа, можемо скористатися цією функцією, для збереження файлу як ASCII текст. Це іноді необхідно, для того, щоб відправляти бінарні (двійкові) файли, коли використовується е - mail застосування старіших версій, які не підтримують цю функцію. При цьому розмір шифрованого файлу збільшується приблизно на 30 відсотків;

– Input Is Text (“вхідний це текст”) – інструктує програму, що початковий файл містить текстову інформацію, а не двійковий код. Використовується тільки в цілях сумісності зашифрованих текстових документів з Unix-системами і їх форматом повернення каретки (перенесенням рядків). Не потрібно відмічати опцію, якщо одержувач файлу не працює на Unix / Linux / Mac і початковий файл не містить звичайний текст;

– Wipe Original (Стирання оригіналу). При виборі цієї опції при шифруванні затиратиметься первинний документ, тепер ніхто, у кого є доступ до жорсткого диска комп'ютера, не зможе відкрити цей файл;

– Conventional Encrypt (стандартне шифрування). При включенні цієї функції користувач покладається на загальну кодову фразу, а не на шифр відкритого ключа. Файл шифрується за допомогою сеансового ключа, який кодує файл з використанням нової фрази.

Тут же є додаткова опція "Self Decrypting Archive - SDA" – архів, що сам розпаковується. Назва цієї опції говорить сама за себе. Тут по аналогії з попередньою функцією використовується стандартне шифрування. При цьому створюється архів з розширенням ".sda.exe". Ця функція дуже схожа на створення "SFX" архівів при архівації звичайними архіваторами, такими як "RAR". В результаті, виконуваний файл може бути розшифрований простим подвійним натисненням мишки на цей файл і введенням кодової фрази. Ця функція розрахована на відправку користувачам, в яких немає комплексу PGP, що робить використання цього продукту мобільнішим і широким у використанні. При використанні цього архіву користувач, що відправляє лист, і той який його отримає, повинні використовувати однакову операційну систему.

Утворений в результаті криптографічного перетворення файл може бути відправлений по відкритих каналах зв'язку. При використанні різних опцій створюється файл з різними іконками, що дозволяє визначити, яку з функцій було використано (рис. 3.14) [63].

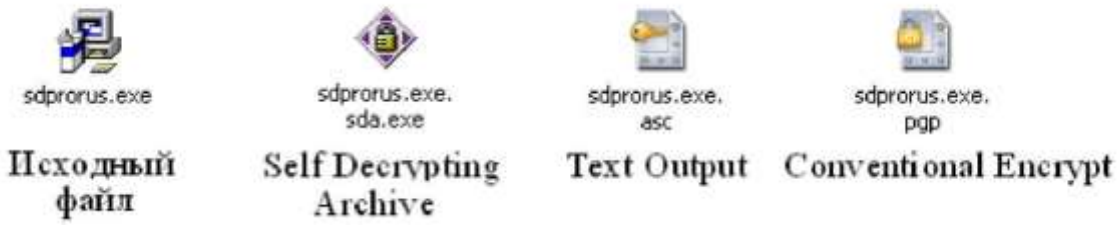

Рисунок 3.14 – Результати криптографічного перетворення

При шифруванні папки, шифрування проходить над кожним файлом, що знаходиться в ній, окремо. Якщо є вкладені папки, PGP обробляє і їх аналогічним чином.

Проте не завжди виникає необхідність повного шифрування даних. Часто відправник і одержувач не хочуть приховувати інформацію від інших користувачів, але бажають, щоб ніхто цю інформацію не міг модифікувати. Для цього і використовується функція генерації електронно-цифрового підпису "Sign", яка додає в початковий каталог цифровий підпис, отриманий за допомогою накладення хеш-функції на початковий файл і зашифровування отриманого хеш-коду відкритим ключем відправника.

При виборі функції "Sign", у вікні "Enter Passphrase" з'явиться 3 опції: "Detached Signature", "Text Output" і "Input is Text". Опція "Detached Signature" в перекладі з англійської означає виготовити "змінний" цифровий підпис. Якщо опція включена (а вона включена по замовчуванню), цифровий підпис буде збережений у вигляді окремого крихітного файлу, що має таке ж ім'я, що і у підписаного файлу, але з розширенням “.sig” (рис. 3.15). Такий файл-підпис можна передавати і публікувати окремо від підписаного, щоб не ускладнювати використання підписаного файлу користувачам, не використовуючим PGP.

Рисунок 3.15 – Формування електронного цифрового підпису

Якщо опцію "Detached Signature" вимкнути, файл буде збережений, як при звичайному шифруванні, і використовувати його без звірки ЕЦП буде неможливо. В тому випадку, якщо відправник зашифровує файл і підпише його, то ЕЦП автоматично буде внесений до файлу, а окремого файлу – підпис з розширенням “*. Sig” не буде [62].

На стороні одержувача зашифровані файли мають бути поміщені в недоступний для інших користувачів каталог, наприклад, "Служебные документы", в якому піддаватимуться операції розшифровки. Щоб розшифрувати документ необхідно на його ярлику клацнути правою клавішею миші, при цьому в спливаючому контекстному меню окрім рядків, стандартних для ОС Windows з'являться ще два рядки: "Decrypt" – розшифрувати і Decrypt/Verify – розшифрувати і верифікувати (перевірити достовірність) документу. Для расшифровування отриманих по мережі файлів досить просто двічі клацнути мишкою по піктограмі цього файлу. Розшифровка даних при цьому здійснюється буквально в одну дію. У випадку якщо файл був зашифрований звичайним способом, без використання функції "Conventional Encrypt", то програма видасть вікно, де визначить, яким ключем був зашифрований файл і запропонує ввести свою (одержувача) ключову фразу, що еквівалентно вступу закритого ключа одержувача.

Рисунок 3.16 – Вікно для введення пароля при розшифровуванні і верифікації файлів

В іншому випадку, якщо файл був зашифрований з використанням функції "Conventional Encrypt", буде видано вікно для вводу також секретної фрази, але без вказування шифру, оскільки файл був зашифрований сеансовим (симетричним) ключем.

Для верифікації незашифрованого файлу, переданого по каналах зв'язку спільно з ЕЦП, достатньо двічі клацнути мишкою по піктограмі ЕЦП, система PGP при цьому також зажадає від одержувача ввести свій секретний пароль. При успішній верифікації (якщо інформація в процесі передачі не була піддана змінам) з'явиться вікно, що інформує одержувача, від кого було отримано істинне (немодифіковане) повідомлення.

3.4 Засоби протидії несанкціонованому доступу

3.4.1 Ідентифікація і аутентифікація користувачів

Для гарантії того, аби лише зареєстровані в АС користувачі могли включити комп'ютер (завантажити операційну систему) і отримати доступ до його ресурсів, кожен доступ до даних в захищеній АС здійснюється в три етапи: ідентифікація — аутентифікація — авторизація. [64]

Ідентифікація — привласнення суб'єктам і об'єктам доступу зареєстрованого імені, персонального ідентифікаційного номера (PIN-коду),

або ідентифікатора, а також порівняння (ототожнення) ідентифікатора, що пред'являється, з переліком привласнених (наявних в АС) ідентифікаторів. Ґрунтуючись на ідентифікаторах, система захисту «розуміє», хто з користувачів в даний момент працює на ПЕОМ або намагається включити комп’ютер (здійснити вхід в систему). Аутентифікація визначається як перевірка приналежності суб'єктові доступу пред'явленого ним ідентифікатора, або як підтвердження достовірності суб'єкта. Під час виконання цієї процедури АС переконується, що користувач, який представився певним легальним співробітником, таким і є. Авторизація — надання користувачу повноважень відповідно до політики безпеки, встановленої в комп'ютерній системі.

Процедури ідентифікації і аутентифікації в захищеній системі здійснюються за допомогою спеціальних програмних (програмно-апаратних) засобів, вбудованих до ОС або ЗЗІ. Процедура ідентифікації проводиться при включенні комп'ютера і полягає в тому, що співробітник «представляється» комп'ютерній системі. При цьому АС може запропонувати співробітнику вибрати своє ім'я із списку зареєстрованих користувачів або правильно ввести свій ідентифікатор. Далі користувач повинен переконати АС в тому, що він дійсно той, ким представився. Аутентифікація в захищених АС може здійснюватися декількома методами [64]:

– парольна аутентифікація (введення спеціальної індивідуальної для кожного користувача послідовності символів на клавіатурі);

– на основі біометричних вимірів (найбільш поширеними методами біометричної аутентифікації користувачів в ЗЗІ є читання папілярного рисунку і аутентифікація на основі вимірів геометрії долоні, рідше зустрічаються голосова верифікація і зчитування райдужної оболонки або сітківки очей);

– з використанням фізичних носіїв аутентифікуючої інформації.

Найбільш простим і дешевим способом аутентифікації особи в АС є введення паролю (важко уявити собі комп'ютер без клавіатури). Проте існування великої кількості різних по механізму дії атак на систему парольного захисту робить її вразливою перед підготовленим зловмисником. Біометричні

методи в ЗЗІ доки не знайшли широкого використання. Безперервне зниження вартості і мініатюризація, наприклад, дактилоскопічних зчитувачів, поява «мишок», клавіатур і зовнішніх флеш-носіїв із вбудованими зчитувачами неминуче приведе до розробки засобів захисту з біометричною аутентифікацією.

В даний час для підвищення надійності аутентифікації користувачів в ЗЗІ застосовують зовнішні носії ключової інформації. В технічній літературі виробники цих пристроїв і розробники систем безпеки на їх основі користуються різною термінологією. Можна зустріти відповідні по контексту терміни: електронний ідентифікатор, електронний ключ, зовнішній носій ключової або кодової (аутентифікуючої) послідовності. Слід розуміти, що це пристрої зовнішньої енергозалежної пам'яті з різним апаратним інтерфейсом, що працюють в режимах зчитування або читання/запис і призначені для зберігання ключової (для шифрування даних) або аутентифікуючої інформації. Найбільш поширеними пристроями є електронні ключі «Touch Memory» на базі мікросхем серії DS199X фірми Dallas Semiconductors. Інша їх назва — «iButton» або пігулки «Далласа» (пристрої випускаються в циліндричному корпусі діаметром 16 мм і завтовшки 3 або 5 мм, рис. 3.17) [64].

Рисунок 3.17 – Зовнішній вигляд електронного ключа iButton і зчитувача інформації

В ЗЗІ активно використовуються пластикові картки різних технологій

(найчастіше із магнітною смугою або проксімі-карти, рис. 3.18). Пластикові картки мають стандартний розмір 54x85,7x0,9 — 1,8 мм.

Рисунок 3.18 – Пластикова карта з магнітною смугою

Зручними для використання в ЗЗІ є електронні ключі eToken (рис. 3.19), виконані на процесорній мікросхемі сімейства SLE66C Infineon, що забезпечує високий рівень безпеки. Вони призначені для безпечного зберігання секретних даних, наприклад, криптографічних ключів. eToken випускається в двох варіантах конструктивного оформлення: у вигляді USB-ключа і у вигляді смарт-карти стандартного формату.

Рисунок 3.19 – Електронні ключі eToken

В більшості програмно-апаратних засобів захисту інформації передбачена можливість здійснювати аутентифікацію особи користувача комбінованим способом, тобто по декількох методах одночасно [54].

Таблиця 3.2 – Варіанти електронних ключів

Модель	Особливість	Рівень	Сертифікат
eToken PRO/32K cert	Сертифікований електронний ключ eToken 3.6, модель eToken PRO у форм-факторі USB-ключа з об'ємом захищеної пам'яті 32КБ	"Конфіденційно", клас захищеності "1Г" (по РД)	№925/5
eToken PRO/64K cert	Сертифікований електронний ключ eToken 3.6, модель eToken PRO у форм-факторі USB-ключа з об'ємом захищеної пам'яті 64КБ	"Конфіденційно", клас захищеності "1Г" (по РД)	№925/5
eToken PRO/SC cert	Сертифікований електронний ключ eToken 3.6, модель eToken PRO у форм-факторі смарт-карти з об'ємом захищеної пам'яті 32КБ	"Конфіденційно", клас захищеності "1Г" (по РД)	№925/5
eToken PRO/SC/64 cert	Сертифікований електронний ключ eToken 3.6, модель eToken PRO у форм-факторі смарт-карти з об'ємом захищеної пам'яті 64КБ	"Конфіденційно", клас захищеності "1Г" (по РД)	№925/5

Комбінування способів аутентифікації знижує ризик помилок, в результаті яких зловмисник може увійти до системи під ім'ям легального користувача.

Для нашого вибору є наступні варіанти (табл. 3.2).

Для своїх потреб будемо використовувати в своїй мережі для ідентифікації та запуску основного комп'ютера електронний ключ Token PRO/32K cert.

3.4.2 Обмеження доступу на вхід в систему

Обмеження доступу до ресурсів АС починається з обмеження фізичного доступу співробітників і «гостей» підприємства в приміщення, в якому розміщуються і функціонують елементи комп'ютерної системи. Цей рубіж захисту організовується шляхом встановлення засобів інженерної закріпленості приміщень, автономних пристроїв охоронної сигналізації, телевізійних систем спостереження, пристроїв захисту робочого місця і безпосередньо ПЕОМ і до функціонування програмних і апаратних ЗЗІ відношення не має [54].

В практиці захисту об'єктів інформатизації під методом «обмеження доступу на вхід в систему» мають на увазі цілий комплекс заходів, що виконуються в процесі завантаження операційної системи. Тому для опису процесу правильного і легального включення комп'ютера фахівці часто використовують термін «довірене завантаження ОС». Правильно організоване довірене завантаження забезпечує виконання 1, 2 і частково третього пунктів вимог до системи захисту інформації наведених вище.

Завдяки процедурам ідентифікації і аутентифікації АС дозволяє подальшу роботу лише зареєстрованим користувачам в іменованому режимі. Проте для цілком довіреного завантаження цього не вистачає. Безпечний вхід в комп’ютерну систему включає також процедуру обмеження доступу по даті і часу, процедуру перевірки цілісності системного програмного забезпечення і апаратури, а також захист від завантаження ОС із змінних носіїв і входу в АС в незахищеному режимі. Перший з цих заходів окрім підтримки дисципліни (що необхідно на підприємстві, де обробляється інформація обмеженого доступу) забезпечує додатковий захист від зловмисників, що намагаються атакувати АС в неробочий час.

Однією зі вбудованих в програмно-апаратне середовище самого комп’ютера процедур обмеження логічного доступу є операція введення паролю BIOS при включенні ПЕОМ. Аби зрозуміти, яке місце в комплексі захисних заходів займає парольний захист, розглянемо процес завантаження персонального комп'ютера без використання ЗЗІ (рис. 3.20) [54].

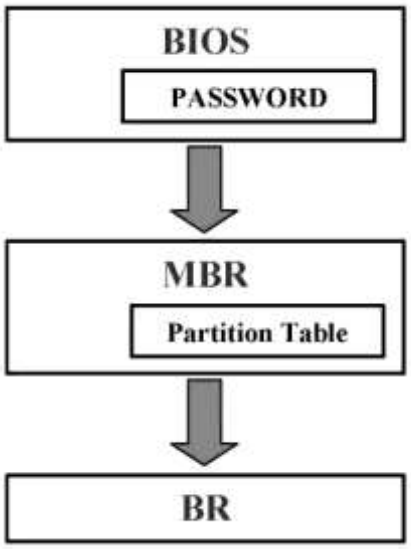

Рисунок 3.20 – Процес стандартного завантаження персонального комп'ютера

При включенні живлення керування ПЕОМ бере на себе програма, записана в ПЗП BIOS, яка проводить процедуру самотестування комп’ютера (Power-On Self-Test, POST). Після тестування з ПЗП BIOS в оперативну пам'ять ПЕОМ завантажується вміст першого сектора нульового циліндра нульової сторони накопичувача на жорсткому магнітному диску (НЖМД). В даному секторі НЖМД знаходиться головний завантажувальний запис (Master Boot Record — MBR), на який передається керування комп'ютером. Програма первинного завантаження (Non-System Bootstrap — NSB — несистемний завантажувач) є першою частиною MBR. NSB аналізує таблицю розділів жорсткого диска (Partition Table), що є другою частиною MBR, і визначає по ній розташування (номери сектора, циліндра і сторони) активного розділу, що містить робочу версію ОС. Визначивши активний (завантажувальний) розділ НЖМД, програма NSB зчитує його нульовий сектор (Boot Record — BR — завантажувальний запис) і передає їй керування ПЕОМ. Алгоритм роботи завантажувального запису залежить від операційної системи, але зазвичай полягає в запуску безпосередньо операційної системи або програми — завантажувача ОС [53].

Парольна система BIOS має лише два варіанти паролів з категоріями

«користувач» і «суперкористувач». Введення парольної інформації виконується (якщо функція активована у відповідних налаштуваннях BIOS) до звернення до жорсткого диска комп'ютера, тобто до завантаження операційної системи. Це лише один із ешелонів захисту АС, який здатний розділити потенційних користувачів на легальних (своїх, що знають пароль користувача) і нелегальних. Парольна система BIOS не забезпечує ідентифікації конкретного користувача.

Захист від входу в АС в незахищеному режимі є дуже серйозною мірою, що забезпечує безпеку інформації і протидіючою спробам підготовлених порушників запустити комп'ютер в обхід системи захисту. Цілісність механізмів захисту може бути порушена, якщо зловмисник має можливість завантажити на комп'ютері будь-яку операційну систему із зовнішнього носія або встановлену ОС в режимі захисту від збоїв. Небезпека завантаження ОС в режимі захисту від збоїв полягає в тому, що завантажується лише обмежений перелік системних драйверів і додатків, у складі яких можуть бути відсутніми модулі ЗЗІ. Конфіденційні дані при неактивному ЗЗІ можуть виявитися абсолютно незахищеними, і зловмисник може отримати до них необмежений доступ [53].

Для протидії подібній загрозі необхідно, по-перше, зробити недоступним для перегляду вміст дисків при завантаженні ОС із зовнішнього носія. Дане завдання може бути вирішене шляхом криптографічного перетворення інформації на жорсткому диску. Зашифрованим має бути не лише вміст конфіденційних файлів, але і вміст виконуваних та інших файлів, а також службові області машинних носіїв.

По-друге, слід внести зміни в стандартний процес завантаження комп'ютера, впровадивши в нього процедури ініціалізації механізмів захисту ще до завантаження ОС. Запуск захисних механізмів ЗЗІ зазвичай виконується по одному з наступних способів: з використанням власного контролера ЗЗІ або шляхом модифікації головного завантажувального запису.

При реалізації першого способу ЗЗІ має бути програмно-апаратним

комплексом і містити власний контролер, який зазвичай встановлюється в слот ISA або PCI. В процесі виконання процедури POST після перевірки основного обладнання BIOS комп'ютера починає пошук зовнішніх ПЗП в діапазоні адрес від C800:0000 до E000:0000 з кроком в 2Kb. Апаратна частина ЗЗІ має бути організована так, щоб її ПЗП, яка містить процедури ідентифікації та аутентифікації користувачів, виявлялось комп'ютерною системою по одній із адрес, що перевіряються системою. При виявленні зовнішнього ПЗП POST BIOS передає керування програмі, розташованої в знайденому ПЗП. Таким чином, захисні механізми (процедури ідентифікації і аутентифікації, контролю цілісності і т. п., записані в ПЗП контролера ЗЗІ) починають працювати ще до завантаження ОС. І лише після вдалого відробітку механізмів захисту засіб захисту повертає керування процедурі POST, або безпосередньо передає керування на MBR жорсткого диска. Окрім ПЗП, що зберігає програми захисних механізмів, у складі ЗЗІ мають бути перепрограмовані ПЗП, в які заноситься список зареєстрованих користувачів з образами аутентифікуючої їх інформації і тимчасовими рамками дозволу входу в АС. Одним із прикладів подібної реалізації довіреного завантаження є ЗЗІ НСД «Аккорд-АМДЗ» (рис. 3.21) [54].

Другий спосіб запуску захисних механізмів застосовується в програмних ЗЗІ, прикладами яких є «Страж NT» і «Dallas Lock», які не мають власних апаратних контролерів. Завдання надійного запуску захисних механізмів (до завантаження ОС) вирішується тут шляхом модифікації головного завантажувального запису в процесі встановлення системи захисту. Зазвичай модифікації піддається лише перша частина MBR — програма першочергового завантаження. В процесі ініціалізації ЗЗІ програма первинного завантаження міняється на власну програму засобу захисту, завданням якої є передача управління на програмний код, що реалізовує запуск і відпрацьовування захисних механізмів довіреного завантаження. Після вдалого виконання всіх передбачених процедур ЗЗІ керування ПЕОМ передається або на штатну програму первинного завантаження ОС, яка при встановленні засобу захисту

копіюється в деякий сектор нульової доріжки НЖМД, або безпосередньо на завантажувальний запис активного розділу жорсткого диска (рис. 3.22).

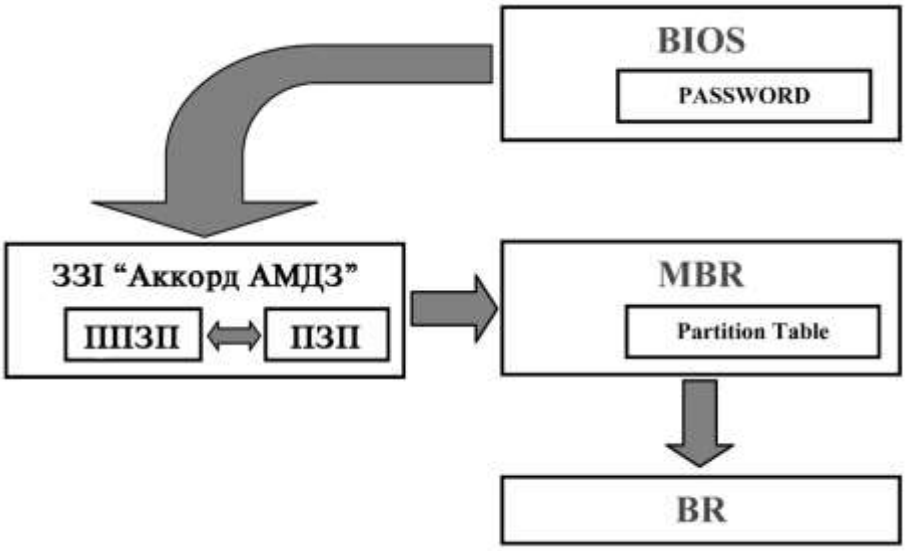

Рисунок 3.21 – Процес завантаження персонального комп'ютера з використанням контролера ЗЗІ

В теорії і практиці забезпечення безпеки АС добре відомий такий спосіб подолання зловмисником системи захисту, як підбір паролю. Він полягає в переборі всіх можливих варіантів паролів («лобова атака») або найбільш ймовірних комбінацій (оптимізований перебір). Для того, щоб унеможливити здійснення штурму парольної системи захисту в ЗЗІ передбачається режим блокування комп'ютера після декількох (зазвичай трьох — п’яти) невдалих спроб введення паролю. Вихід АС з цього режиму можливий лише після виключення живлення (повного перевантаження системи). Режим блокування може бути запущений при виявленні системою захисту будь-яких нештатних дій користувача як під час довіреного завантаження (наприклад, якщо код, записаний в представлену карту пам’яті не відповідає введеному ідентифікатору і паролю), так і під час подальшої роботи (наприклад, при спробі звернутися до заборонених для доступу портам, пристроям вводу-виводу). Природно, всі спроби невдалого входу в систему, що привели до блокування комп'ютера, які фіксуються в спеціальному журналі [54].

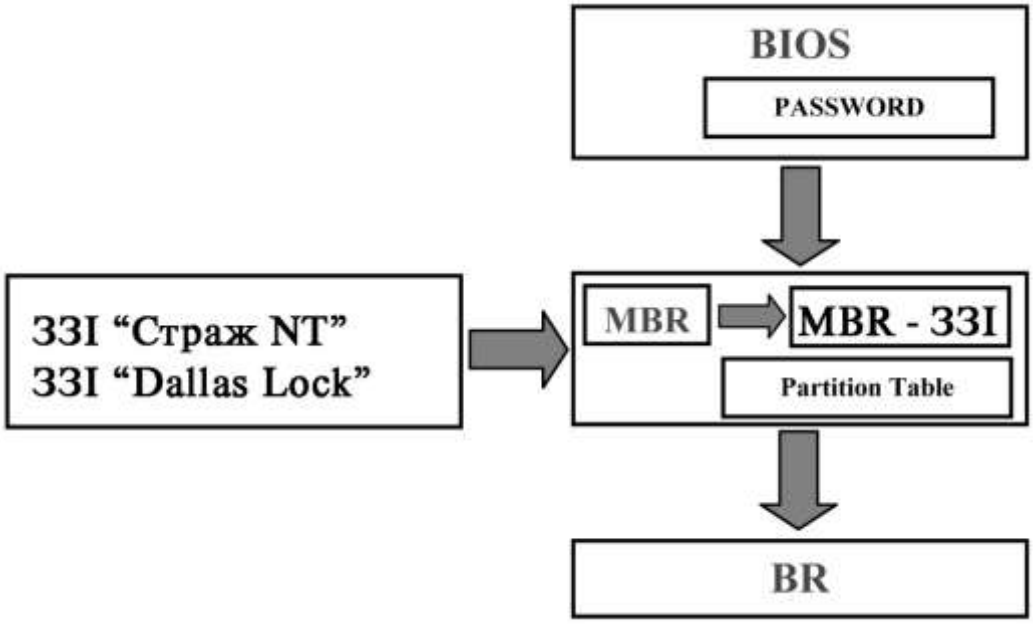

Рисунок 3.22 – Процес завантаження персонального комп'ютера з використанням модифікації MBR

Слід зазначити, що за відсутності у функціональному наборі ЗЗІ процедури шифрування захищуваних даних необхідно забезпечити надійний захист самого комп'ютера від безпосереднього фізичного доступу. Дійсно, якщо зловмисникові вдасться витягувати контролер ЗЗІ слоту ПЕОМ, процес завантаження ОС перестане носити захищений характер, і буде здійснюватися стандартно. За наявності фізичного доступу до елементів АС підготовлений зловмисник може просто вкрасти жорсткий диск і намагатися добути інформацію, що цікавить його, шляхом аналізу НЖМД з потужністю різних низькорівневих редакторів. Заборона входу в систему в обхід механізмів захисту є необхідним складником процесу довіреного завантаження і забезпечує виконання 1, 2 і 3 пунктів вимог до системи захисту інформації.

3.6 Висновки до третього розділу

В даному розділі проведено розробку методики вибору системи захисту інформації, а також проведено вибір методу системи захисту. Проведено аналіз і постановка задачі вибору системи захисту інформації . Описано використання

системи захисту конфіденційної інформації PGP, а зокрема наведено основні характеристики системи PGP, проведено ініціалізацію системи PGP на робочій станції. Описано засоби протидії несанкціонованому доступу.

4 СПЕЦІАЛЬНА ЧАСТИНА

Більшість програмних засобів для пошуку Malware аналізують систему в режимі live, тобто під час її роботи. Але багатьом користувачам не выдомо про існування програм, які, окрім іншого, здатні виконувати так звані офлайн-дослідження, дозволяючи відшукати зловмисне програмне забезпечення в пам'яті комп'ютера, коли до того немає доступу або він взагалі вимкнений.

Віднедавна з’явився новий спосіб пошуку Malware. Основним призначенням цього інструменту є зовсім не пошук руткітів, а комплексний аналіз пам'яті. Але так вийшло, що включені в нього техніки ідеально підходять для того, щоб відшукати добре прихований Malware.

Окрім основної категорії продуктів, призначених для глибокого вивчення дискових накопичувачів, широко використовуються також рішення для аналізу оперативної пам'яті. Такі дослідження виділяють в особливий вид експертиз — Метогу Forensic. Деякі з додатків (в тому числі Memoryze) вміють не лише виконувати дослідження “живої” системи, але й аналізувати образ пам'яті, в який завчасно було поміщено повний вміст оперативної пам'яті комп'ютера. Це дає великий простір для роботи. Маючи такий образ, ніщо не заважає пізніше розібратися, які застосування запущені в системі (на момент створення дампу) або, наприклад, з якими хостами взаємодіють процеси, що цікавлять нас. Це ще й відмінний спосіб для пошуку Malware. Можна зробити дамп на проблемній машині й далі на своєму власному комп'ютері без будь-яких незручностей розбиратися, що завантажено в пам'яті. Тут треба розуміти, що в образ поміщається весь вміст пам'яті, який зчитує і аналізує спеціальний парсер, який обов'язково віднайде шкідливе програмне забезпечення.

Програму Memoryze – найпотужніший засіб аналізу пам'яті, що для багатьох стало частиною джентльменського набору. Розробниками є Джемі

Батлер і Пітер Сілбермен. Що можна отримати, використовуючи Memoryze:

– повний образ всього діапазону системної пам'яті (без використання API-викликів), збережений у файл для подальшого аналізу;

– дамп адресного простору будь-якого процесу, включаючи список завантажених DLL і EXE, купу та стек (цей дамп можна далі досліджувати в дизассемблере);

– образ усіх завантажених драйверів або деяких з них;

– повний список усіх процесів, включаючи приховані руткітами, причому для кожного процесу є можливість визначити всі хендли (наприклад, використовуваних файлів або ключів реєстру), мережеві сокети, імпортовані та експортовані функції і так далі;

– усі строкові змінні, використовувані процесами;

– повний список усіх драйверів, у тому числі ті, які маскуються під Malware;

– перелік усіх модулів ядра;

– перерахування всіх встановлених хуків (вони часто використовуються Malware);

– і багато чого іншого.

В деяких ситуаціях дуже зручно мати програму при собі, тому її найкраще розмістити на флеш-накопичувачі достатнього об’єму, щоб туди помістився ще й створений дамп пам'яті.

Не зайвим буде записати на флешку й файли Audit Viewer'a, щоб відразу мати можливість проаналізувати отриманий дамп або взагалі виконати “живе” дослідження системи.

Memoryze працює з командного рядка. Але для більшої зручності із програмою поставляють декілька batch-скриптів для виконання найбільш типових завдань. Так, для отримання образу з повним вмістом оперативної пам'яті є сценарій MemoryDD.bat, який в подальшому будемо використовувати. Після запуску він генерує конфігурацію з налаштуваннями та виконує

memoryze.exe з потрібними параметрами: “G:\\\\memoryze\\\\MemoryDD.bat”. Після виконання команди є два варіанти: програма успішно створить дамп із пам'яттю або в неї нічого не вийде. Останнє дуже ймовірно. Справа в тому, що для роботи Memoryze використовує kernel-mode драйвер, що надає програмі прямий доступ до пам'яті. Немає драйвера - немає дампа. Є кілька причин, по яких драйвер не зможе завантажитися, але в першу чергу — через відсутність прав адміністратора. Тому варто переконатися, що запускаєш її з адміністраторського командного рядка. Інша поширена причина — антивірус, який може перешкоджати прямому звертанню до пам'яті. Можливо, що на певний час його прийдеться відключити. Якщо все пройде успішно, отриманий дамп буде збережений у папці з вихідними результатами (по замовчуванню в папці з Memoryze\Auditsl. Структура каталогу влаштована таким чином, щоб повторні виконання процедури не перезаписували раніше отримані образи. Так що завжди легко визначити, на якому комп'ютері й коли був створений образ.

Для аналізу та перегляду образу пам'яті використовується інша утиліта — Audit Viewer. Причому вміст оперативної пам'яті необов'язково повинен бути скопійований за допомогою Memoryze. Набагато більшого значення має операційна система, на якій створювався образ. Причиною тому є структури пам'яті, які можуть значно відрізнятися від однієї версії операційної системи до іншої. У деяких випадках навіть один встановлений (або, навпаки, невстановлений) патч може впливати на можливість виконати аналіз даних. Аналізатор може парсити тільки структури відомої йому ОС. Тому, перш ніж говорити, що Memoryze і Audit Viewer не працюють, необхідно переконатися, що користувач не намагається виконати аналіз непідтримуваної системи (наприклад, Windows XP SP1). На щастя, для значного списку ОС все повинно без проблем вийти:

- Windows 2000 Service Pack 4 (32-bit);
- Windows XP Service Pack 2 and Service Pack 3 (32-bit);
- Windows Vista Service Pack 1 and Service Pack 2 (32-bit);
- Windows 2003 Service Pack 2 (32-bit);

– Windows 2003 Service Pack 2 (64-bit);
– Windows 7 Service Pack 0 (32-bit);
– Windows 7 Service Pack 0 (64-bit);
– Windows 2008 Service Pack 1 and Service Pack 2 (32-bit);
– Windows 2008 R2 Service Pack 0 (64-bit).

Для аналізу дампу достатньо запустити auditviewer.exe і вибрати пункт “Configure Memoryze”. Не звертаємо уваги на опцію “Ореп Existing Results” — вона призначена для повторного відкриття вже існуючого файлу з аналізом дампу. Для виконання дослідження програма попросить вказати шлях до виконуваного файлу Memoryze і вибрати папку для збереження результатів. Далі є два варіанти: виконати аналіз наявного дампу пам'яті (можливо, із зовсім іншого комп'ютера) або проаналізувати пам'ять із поточного комп'ютера. Вибираємо перший режим і вказуємо шлях до img-файлу з нашим образом.

Кілька наступних кроків майстра необхідні для того, щоб вказати, що саме нас цікавить і наскільки повну інформацію прагнемо одержати. Скажемо, якщо цікавлять тільки драйвери, які працюють у системі, можна не парсити інформацію про хуки й процеси. Підхід “поставити всі галочки” тут не пройде. Важливо зрозуміти просту річ: чим детальніше аналіз буде виконувати Audit Viewer, тим довше вона буде це робити. В деяких випадках процес може затягтися на цілий день. Але такого можна уникнути, мінімізуючи кількість перевірок, які буде виконувати програма. Наприклад, включена опція для добування рядкових змінних (“Extract strnigs”) неодмінно приведе до багатогодинного аналізу. Тому цей вид дослідження рекомендується залишити на повторний прохід (якщо такий знадобиться), виконавши в перший раз тільки ті перевірки, які дійсно потрібні. Гарні результати при високій швидкості сканування можуть дати наступні настройки сканування: режим дослідження процесів (“Process Enumiration”) без визначення хуків і драйверів, але з більшістю включених опцій за винятком вже згаданої “Extract Strings”. Окремо йдуть опції для добування “Acquisition” з пам'яті або образу пам'яті адресного

простору драйверів або процесів. В основному це потрібно, якщо користувач має конкретні наміри досліджувати щось із видобутих дампів в дизасемблері.

Як тільки всі налаштування аналізу будуть задані, Audit Viewer почне роботу, відобразивши на екрані прогрес-бар. У вікні програми прямо під час парсингу дампа пам'яті будуть відображатися результати аналізу, включаючи інформацію про процеси, драйвери, хуки (залежно від обраних налаштувань). Отут прийдеться почекати, але зате звіт тебе неодмінно впечатлит. Чого вартий тільки список ідентифікованих процесів зі списком усіх зв'язаних DLL**,** хендлів, секцій пам'яті і так далі. Це буде список абсолютно всіх процесів, включаючи ті, які, можливо, приховані в системі руткітами. Та ж історія і з драйверами.

Розглянемо випадок, коли можна проаналізувати пам'ять на наявному в розпорядженні комп'ютері. В цьому випадку необов'язково створювати дамп — в Audit Viewer є live-режим, який має ряд переваг. Найголовніша перевага в тому, що крім безпосередньо оперативної пам'яті можна підключити для аналізу ще й swap-файл, а також виконати перевірку цифрових підписів. Ця інформація використовується для підрахунку індексу MRI (Memoryze's Malware Rating), що дозволяє швидко визначити широке коло Malware. Якщо програмі якийсь компонент здасться підозрілим, то про це стане відразу відомо. Потрібно мати на увазі, що при відповідній включеній опції утиліта буде обчислювати хеш для кожного файлу, що виконується, і бібліотеки, асоційованих із запущеними процесами. Це може забрати значний час. Тому як мінімум не треба вибирати підрахунок усіх хешів відразу (підтримуються MD5, SHA1, SHA256). Можна обмежитися одним з них, який дійсно будемо використовувати: наприклад, MD5. Виконання “живого” аналізу мало чим відрізняється від парсингу дампа пам'яті. В тому місці, де раніше вказували шлях до img-файлу, досить вибрати режим “Acquire (and/or) Analyze Live Метогу”. І все. Виконання “живого” аналізу ніяк не заважає зробити дамп пам'яті. Ніколи свідомо не знаєш, що пізніше можна у ньому виявити й побачити. Для цього в момент вибору режимів добування (там же, звідки

раніше могли витягти дамп конкретного процесу або драйвера) треба не забути вибрати опцію “Memory Acquisition”.

Зв'язування Memoryze і Audit Viewer не єдина для проведення Memory Forensic. Широко поширений також відкритий проект Volatility Framework. При наявності MiniGW і інтерпретатора Python його навіть можна запустити під Windows, але для цього прийдеться постаратися. Набагато простіше користуватися ним під Linux. В спеціальному дистрибутиві для комп'ютерних криміналістів SANS Investigative Forensic Toolkit фреймворк включений і відразу готовий до роботи. Зборка цієї системи викладена у вигляді образу для запуску під Vmware.

Взагалі, сама тема Метогу Forensic викликає великий інтерес, причому не тільки як окремий вид досліджень, але і як ефективний спосіб для аналізу системи (часто непомітного). Це, до того ж, що ще й працює метод для лікування й реверсингу із цільового комп'ютера окремих процесів і драйверів.

5 ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від оптимізації системи захисту локальної мережі з використанням серверів Sun Microsystems, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільність впровадження відповідної розробки.

Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції, що мала місце при проведенні наукових досліджень.

5.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Витрати праці на підготовку опису задачі	інженер	20
2.	Витрати праці на розробку проекту	інженер	35
3.	Витрати праці на розробку структури системи	інженер	20
4.	Витрати праці на створення системи по вибраному проекту та структурі	інженер	115
5.	Витрати праці на підготовку документації	інженер	25

Продовження таблиці 5.1

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
6.	Витрати праці на відлагодження роботи спроектованої системи при комплексній відладці	інженер	20
Разом			**235**

Сумарний час на проведення науково-дослідної роботи становить 235 годин.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Рекомендовані тарифні ставки: керівник проекту – 40,5...72,0 грн./год., інженер – 27,0...45,0 грн./год., консультант – 31,5...49,5 грн./год., технік – 27,0...40,5 грн./год., лаборант – 18,0...31,5 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г, \quad (5.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в даному дослідженні виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 45 \cdot 235 = 10575 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод.} = 10575 \cdot 0{,}15 = 1586{,}25 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($B_{о.п.}$) визначаються за формулою:

$$B_{о.п.} = З_{осн.} + З_{дод.}. \quad (5.3)$$

$$B_{о.п.} = 10575 + 1586{,}25 = 12161{,}25 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

1) фонд страхування на випадок безробіття – 1,3 %;
2) фонд по тимчасовій втраті працездатності – 2,9 %;
3) пенсійний фонд – 32,3 %.

У сумі зазначені відрахування становлять 37,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{с.з.} = ФОП \cdot 0{,}375, \quad (5.4)$$

де $ФОП$ – фонд оплати праці, грн.

$$B_{с.з.} = 12161{,}25 \cdot 0{,}375 = 4560{,}47 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 5.2.

Таблиця 5.2 – Зведені розрахунки витрат на оплату праці

№ п/п	**Категорія працівник-ків**	**Основна заробітна плата, грн.**			**Додаткова заробітна плата, грн.**	**Нарахув. на ФОП, грн.**	**Всього витрати на оплату праці, грн. *6=3+4+5***
		Тарифна ставка, грн.	**К-сть відпра-цьов. год.**	**Фактично нарах. з/пл., грн.**			
А	*Б*	*1*	*2*	*3*	*4*	*5*	*6*
1	інженер	45	235	10575	1586,25	4560,47	16721,72

Сумарні затрати на оплату праці становлять 16721,72 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{B\,i} = q_i \cdot p_i, \tag{5.5}$$

де: q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{B\,i}. \tag{5.6}$$

Проведені розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	**Одиниця виміру**	**Норма витрат**	**Ціна за одиницю, грн**	**Затрати матеріалів, грн**	**Транспортно-заготівельні витрати, грн**	**Загальна сума витрат на матеріали, грн**
1. Основні матеріали						
Програмне забезпечення різного рівня	комплект	1	20538	–	–	20538
Разом:						20538

Сумарні матеріальні затрати становлять 20538 грн.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S \ , \tag{5.7}$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (0,714 грн. з ПДВ за 1 кВт).

Потужність комп'ютера для проведення дослідження – 720 Вт, кількість годин роботи обладнання згідно таблиці 5.1 – 235 годин.

Тоді, $З_е = 0{,}72 \cdot 235 \cdot 0{,}714 = 120{,}81$ грн.

5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А = \frac{Б_В \cdot Н_А}{100\%}, \tag{5.8}$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Для даного дослідження засобом роботи є комп'ютер. Його сума становить 10250 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{10250 \cdot 5\%}{100\%} = 512{,}5 \text{ грн.}$$

Оскільки робота виконувалась 235 годин, то амортизаційні відрахування будуть становити:

$$A = \frac{512{,}5 \cdot 235}{150} = 802{,}92 \text{ грн.}$$

5.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6, \qquad (5.9)$$

де $Н_В$ – накладні витрати.

Отже, накладні витрати:

$$H_в = 12161{,}25 \cdot 0{,}3 = 3648{,}38 \text{ грн.}$$

5.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	**Сума, грн.**	**В % до загальної суми**
Витрати на оплату праці (основну і додаткову заробітну плату)	12161,25	29,07
Відрахування на соціальні заходи	4560,47	10,90
Матеріальні витрати	20538	49,10
Витрати на електроенергію	120,81	0,29
Амортизаційні відрахування	802,92	1,92
Накладні витрати	3648,38	8,72
Собівартість	**41831,83**	**100**

Собівартість (C_B) НДР розрахуємо за формулою:

$$C_B = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + A + H_в. \quad (5.10)$$

Отже, собівартість дослідження дорівнює:

$$C_B = 12161{,}25 + 4560{,}47 + 20538 + 120{,}81 + 802{,}92 + 3648{,}38 = 41831{,}83 \text{ грн.}$$

В результаті проведених розрахунків собівартість науково-дослідної роботи становить 41831,83 грн.

5.8 Розрахунок ціни науково-дослідної роботи

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_В \cdot (1 + P_{рен}) + К \cdot B_{н.і.}}{К} \cdot (1 + ПДВ), \quad (5.11)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

$К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

$ПДВ$ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти $К$ та $B_{і.н}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни НДР буде мати вигляд:

$$Ц = C_В \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.12)$$

Звідси ціна на НДР складе:

$$Ц = 41831{,}83 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 65257{,}65 \text{ грн.}$$

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = \frac{П}{C_В}, \tag{5.13}$$

де $П$ – прибуток;

$C_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_В. \tag{5.14}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 65257{,}65 - 41831{,}83 = 23425{,}82 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{Св}. \tag{5.15}$$

Тоді, $E_р = \frac{23425{,}82}{41831{,}83} = 0{,}559$.

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_р = \frac{1}{E_р}, \tag{5.16}$$

Термін окупності дорівнює:

$$T_p = \frac{1}{0{,}559} = 1{,}78 \text{ року.}$$

5.10 Висновки до п’ятого розділу

В цьому розділі дипломної роботи було розраховано основні техніко-економічні показники дослідження (див. таблицю 5.5).

Розраховане значення економічної ефективності становить 0,559, що є високим значенням.

Так само нормальним є термін окупності. Для даного дослідження він становить 1.78 року.

Таблиця 5.5 – Техніко-економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	41831,83
2.	Плановий прибуток, грн.	23425,82
3.	Ціна, грн.	65257,65
4.	Економічна ефективність	0,559
5.	Термін окупності, рік	1,78

Отже, дане дослідження може бути впроваджене та мати подальший розвиток, оскільки воно є економічно вигідним за всіма основними техніко-економічними показниками.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

6.1.1 Завдання керівника підприємства в охороні праці

Створення служби охорони праці на підприємствах будь-якої форми власності передбачено Законом України «Про охорону праці» і є обов'язком роботодавця, якщо кількість найманих працівників складає 50 і більше осіб. Діє така служба на підставі Типового положення, затвердженого Державним комітетом України з нагляду за охороною праці (Наказ від 15.11.2004 р. № 255). Підпорядковується служба охорони праці безпосередньо роботодавцю. На підставі Типового положення з урахуванням специфіки виробництва, видів діяльності, кількості працівників, умов праці та інших факторів роботодавець розробляє Положення про службу охорони праці відповідного підприємства.

На підприємстві з кількістю працівників менше 50 створення цілої служби не є обов'язковим і доцільним. Її функції можуть виконувати за сумісництвом особи, які мають відповідну підготовку та освіту – фахівці або інженери з охорони праці.

В організаціях з кількістю працівників менше 20 для виконання функцій служби охорони праці можуть залучатися фахівці на договірній основі. При цьому він повинен мати стаж роботи не менше 3 років і пройти навчання з охорони праці.

Керівники та спеціалісти служби охорони праці за своєю посадою і заробітною платою прирівнюються до керівників і спеціалістів основних виробничо-технічних служб.

Основні завдання служби охорони праці [62]

Згідно з Типовим положенням на службу охорони праці підприємства покладаються такі завдання:

– відпрацювання ефективної системи управління охорони праці на підприємстві та сприяння вдосконаленню діяльності в цьому напрямку кожного структурного підрозділу і кожного працівника;

– забезпечення професійної підтримки рішень роботодавця щодо цих питань;

– організація проведення профілактичних заходів, спрямованих на усунення шкідливих і небезпечних виробничих факторів, запобігання нещасним випадкам на виробництві, професійним захворюванням та іншим випадкам загрози життю або здоров'ю працівників;

– вивчення та сприяння впровадженню у виробництво досягнень науки і техніки, прогресивних і безпечних технологій, сучасних засобів колективного та індивідуального захисту працівників;

– контроль за додержанням працівниками вимог законів та інших нормативно-правових актів з охорони праці, положень (за наявності) галузевої угоди, розділу «Охорона праці» колективного договору та актів з охорони праці, що діють у межах підприємства.

– інформування та надання роз'яснень працівникам підприємства з питань охорони праці.

Функції служби охорони праці [62]

Для виконання передбачених законодавством завдань органи охорони праці на підприємстві:

– розробляють спільно з іншими підрозділами комплексні заходи, плани, програми з поліпшення умов праці, запобігання виробничому травматизму і професійних захворювань;

– готують проекти наказів з питань охорони праці і подають їх на розгляд роботодавцю;

– проводять перевірки дотримання працівниками нормативно-правових актів з охорони праці;

– складають звітність з охорони праці;

– проводять з працівниками інструктажі з охорони праці;

– ведуть облік та аналізують причини виробничого травматизму;

– забезпечують належне оформлення та зберігання документації з питань охорони праці, а також своєчасну передачу її в архів для тривалого зберігання;

– складають за участю керівників підрозділів підприємства переліки професій, посад і видів робіт, щодо яких повинні бути розроблені інструкції з охорони (безпеки) праці, надають допомогу під час їх розроблення;

– інформують працівників про основні вимоги законів, інші нормативно-правових акти та акти з охорони праці, що діють у межах підприємства.

Крім того, функціями служб і спеціалістів з охорони праці є розгляд питань про підтвердження наявності небезпечної виробничої ситуації, яка стала причиною відмови працівника від виконання дорученої роботи, листів, заяв, скарг працівників підприємства, що стосуються питань дотримання законодавства про охорону праці [63].

Служба охорони праці на підприємстві повинна забезпечити підрозділи нормативно-правовими актами з охорони праці, що діють у межах підприємства, посібниками, навчальними матеріалами з цих питань; організовувати роботу кабінету з охорони праці, наради, семінари та інші заходи з цих питань.

Однією з найважливіших функцій, які покладені на службу охорони праці, є участь у розслідуванні нещасних випадків, професійних захворювань і аварій на виробництві. Також фахівці з охорони праці беруть участь у складанні

санітарно-гігієнічної характеристики робочих місць працівників, які проходять обстеження щодо профзахворювань; у проведенні внутрішнього аудиту охорони праці та атестації робочих місць на відповідність нормативно-правовим актам з охорони праці; у складанні списків професій і посад, згідно з якими працівники повинні проходити обов'язкові попередні та періодичні медичні огляди; в організації навчання з питань охорони праці та роботи комісії з перевірки знань з цих питань [63].

Повноваження служби охорони праці [62]

Служба охорони праці на підприємстві покликана також контролювати дотриманням вимог роботодавцем законодавства з охорони праці, тому має право видавати керівникам структурних підрозділів підприємства обов’язкові для виконання приписи щодо усунення наявних недоліків і отримувати від них необхідні відомості, документацію і пояснення з питань охорони праці. Припис спеціаліста з охорони праці може скасувати лише роботодавець. Припис складається у двох примірниках, один з яких видається керівнику робіт, об'єкта, цеху, другий залишається і реєструється в службі охорони праці і зберігається протягом 5 років. Якщо керівник структурного підрозділу підприємства відмовляється від підпису в отриманні припису, спеціаліст охорони праці направляє відповідне подання на ім'я особи, якій адміністративно підпорядкований цей структурний підрозділ, або роботодавцю.

Також служба охорони праці має право [62]:

– зупиняти роботу виробництв, ділянки, машин, механізмів, устаткування у разі порушень, які створюють загрозу життю або здоров’ю працівників;

– вимагати відсторонення від роботи осіб, які не пройшли передбачених законодавством медичного огляду, навчання, інструктажу, перевірки знань і не мають допуску до відповідних робіт або не виконують вимоги нормативно-правових актів з охорони праці;

– надсилати роботодавцю подання про притягнення до відповідальності посадових осіб і працівників, які порушують вимоги щодо охорони праці;

– за поліпшення стану безпеки праці вносити пропозиції про заохочення працівників за активну роботу;

– залучати, за погодженні з роботодавцем і керівниками підрозділів підприємства, фахівців підприємства для проведення перевірок стану охорони праці.

Як бачимо, створення служби охорони праці на підприємстві важливо не лише для того, щоб виконати вимоги законодавства в цій сфері, але і мінімізувати ризики відповідальності роботодавця за порушення вимог безпеки праці, а також виконувати низку інших важливих функцій: вести документацію з питань охорони праці, проводити інструктажі, перевіряти знання та ін.

6.1.2 Професійні захворювання працівників галузі інформаційних технологій

За даними рекрутингових агентств експерти склали рейтинг спеціальностей, які користуються найбільшим попитом в Україні. Перше місце у цьому рейтингу займають IT-інженери та програмісти [64]. Ця галузь є однією з тих, які дуже стрімко розвиваються, в неї інвестуються великі кошти, та вона приносить ще більші прибутки. Якщо ж абстрагуватися від фінансів, то IT-сфера просто дуже цікава для вивчення. Але попри низку переваг, як і кожна професія, професія програміста має і свої недоліки. Зараз ми розглянемо ті з них, які пов‘язані безпосередньо зі здоров‘ям. Але ще одна ремарка з мого боку, перш ніж ми перейдемо до суті: хоча програмісти, «хакери» або інші IT-шники не є одними й тими самими поняттями, але за часом роботи за комп‘ютером усі ці професії чимось подібні між собою, тому на час моєї доповіді вважатимемо терміни «програміст», «IT-шник» та інші синонімами.

Професійні захворювання користувачів в галузі інформаційних технологій зумовлені дією шкідливих виробничих факторів, серед основних із них виділяють наступні [65]:

- сидяче положення протягом тривалого часу;
- вплив електромагнітного випромінювання монітора;
- втома очей, навантаження на зір;
- перевантаження суглобів кистей;
- стрес при втраті інформації.

Сидяче положення. Поза, в якій сидить людина за комп'ютером є для організму вимушеною і неприємною: напружені шия, м'язи голови, руки і плечі, в результаті чого з’являється зайве навантаження на хребет, у дорослих це призводить до остеохондрозу, а в дітей – до сколіозу.

У тих, хто багато сидить, між сидінням стільця і тілом утвориться свого роду тепловий компрес, що призводить до застою крові в тазових органах, як наслідок – простатит і геморой, гінекологічні хвороби. Крім того, малорухомий спосіб життя часто приводить до ожиріння.

Втома очей, навантаження на зір. Очі реєструють найменшу вібрацію тексту чи малюнку, а тим більше мерехтіння екрана. Перевантаження очей приводить до втрати гостроти зору. Погано позначаються на зорі невдалий підбор кольору, шрифтів, компонування вікон у використовуваних програмах, неправильне розташування екрана.

В осіб, які працюють на сучасній обчислювальній техніці, може виникнути астенопія – це будь-які суб'єктивні зорові симптоми або емоційний дискомфорт, що є результатом зорової діяльності. Симптоми астенопії: пелена перед очима, двоїння, блимання; відчуття втоми очей, підвищення температури, печіння, почервоніння, біль в очах; головний біль та ін.[65]

Більш чутливими до виникнення астенопії є люди з порушеннями зору. Важливу роль у розвитку астенопії відіграє якість зображення інформації на

моніторі. Так, симптоми астенопії у користувачів ПК більшою мірою проявляються після 60 хв роботи за екраном при частоті регенерації 30 Гц, ніж після роботи такий самий час при частоті регенерації 60 Гц, тобто при стабільному зображенні тексту. Дефекти фокусування і розпливчасті символи на екрані посилюють астенопію. Зоровий дискомфорт частіше виникає при великій відмінності яскравості екрана і паперового документа. Відомі дані про можливість виникнення катаракти в осіб, які працюють з моніторами на основі ЕПТ.

Встановлено також, що жінки частіше, ніж чоловіки, скаржаться на зоровий дискомфорт. У жінок віком 31…45 років астенопія виникає частіше, ніж у жінок віком 18…30 років, що свідчить про вплив на розвиток астенопії стажу роботи. На зорову втому скаржаться 47 % користувачів ПК, які працюють безперервно менше 30 хв, і 66 % користувачів, які працюють понад 30 хв. Ці симптоми більшою мірою виявляються в осіб, які менше контролюють свою роботу, працюють з великим напруженням і не задоволені роботою.

Зафіксовані випадки кольорової зорової післядії в операторів (ефект Мак-Галоха). Оператори, які працювали з дисплеєм із зеленими знаками на темному фоні, бачили потім рожеве фарбування білих предметів. Цей ефект може зберігатися протягом дня і довше. Частота таких порушень варіює від 5 – 8 % до 63 – 90 % в залежності від виду виконуваної роботи.

У 80 % працівників при напруженій зоровій роботі спостерігається прогресуюче зниження працездатності, що настає через 45…60 хв і поступово призводить до перевтоми, розладів центральної нервової та інших систем організму. У другій половині дня (іноді раніше) з'являються загальна втома, головний біль, біль в очах. Латентний період зорово- і акустико-моторної реакцій до закінчення зміни подовжується відповідно на 14 та 20 %; швидкість опрацювання інформації зменшується на 25…34 %; стійкість ясного бачення знижується на 40…52 %. Під кінець робочого дня частішають серцеві скорочення і підвищується систолічний та діастолічний артеріальний тиск [65].

Перевантаження суглобів кистей рук. У користувачів ПК вимушена робоча поза і виконання дрібних стереотипних рухів призводять до кістково-м'язового дискомфорту. Виявляються такі симптоми, як біль у кістках, скутість м'язів, відчуття втоми, судоми, оніміння та тремтіння рук. Перелічені симптоми локалізуються в різних частинах тіла (шиї, плечах, руках та ін.) і виникають з різною частотою (щодня, епізодично або рідко). Частота подібних скарг користувачами ПК залежить від їхнього віку, статі і тривалості роботи за комп'ютером. Нервові закінчення подушечок пальців травмуються від постійних ударів по клавішах, виникають оніміння, слабкість, у подушечках “бігають мурашки”. Це може привести до ушкодження суглобного і зв'язкового апарата кисті, а надалі захворювання кисті можуть стати хронічними.

Неправильне положення рук може призвести до виникнення такого захворювання кистей, зап'ясть і ліктів як RSI, (repetitive strain injury), "травма від постійної напруги". Проявляється RSI по-різному, найчастіше болем в ураженій руці, але нерідко і сверблячкою, онімінням, набряками, набряканням. Біль та інші явища можуть іноді локалізуватися, іноді блукати по руці від фаланг пальців до плеча. У США це захворювання до того, як термін RSI прижився, найчастіше називали carpal tunnel syndrome (синдром карпального каналу або кистьовий тунельний синдром), а в Україні ставили діагноз тендоніт – запалення сухожиль.

Стрес від втрати інформації. Далеко не всі користувачі регулярно роблять резервні копії своєї інформації. Але ж і віруси не дрімають, і вінчестери кращих фірм, буває, ламаються, і навіть найдосвідченіший програміст може іноді натиснути не ту кнопку. За даними ВОЗ, в операторів і представників інших професій, які працюють з ПЕОМ, внаслідок стресу виникають психічні порушення. Такі розлади, як тривога, дратівливість і пригніченість, проявляються у 25…70 % операторів. Дуже часто спостерігаються безсоння і втрата апетиту; психосоматичні симптоми (серцебиття, біль у грудях, запор та інші порушення нижнього відділу

шлунково-кишкового тракту) з'являються у 15…50 % операторів. У результаті такого стресу зустрічались випадки й інфаркту.

6.2 Безпека в надзвичайних ситуаціях

6.2.1 Застосування основних способів та засобів в ході проведення невідкладних аварійно-рятувальних робіт на промисловому підприємстві

1. Проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій у мирний час та в особливий період включає:

– організацію та управління аварійно-рятувальними та іншими невідкладними роботами;

– розвідку районів, зон, ділянок, об’єктів проведення робіт з ліквідації наслідків надзвичайної ситуації;

– визначення та локалізацію зони надзвичайної ситуації;

– виявлення та позначення районів, які зазнали радіоактивного, хімічного забруднення чи біологічного зараження (крім районів бойових дій);

– прогнозування зони можливого поширення надзвичайної ситуації та масштабів можливих наслідків;

– ліквідацію або мінімізацію впливу небезпечних чинників, які виникли внаслідок надзвичайної ситуації;

– пошук та рятування постраждалих, надання їм екстреної медичної допомоги і транспортування до закладів охорони здоров’я;

– евакуацію або відселення постраждалих;

– виявлення та знешкодження вибухонебезпечних предметів;

– санітарну обробку населення та спеціальну обробку одягу, техніки, обладнання, засобів захисту, будівель, споруд і територій, які зазнали радіоактивного, хімічного забруднення чи біологічного зараження;

– надання медичної допомоги постраждалим, здійснення санітарнопротиепідемічних заходів, забезпечення санітарного та епідемічного благополуччя населення в районі виникнення надзвичайної ситуації та місцях тимчасового розміщення постраждалих;

– запровадження обмежувальних заходів, обсервації та карантину;

– надання психологічної та матеріальної допомоги постраждалим, проведення їх медико-психологічної реабілітації;

– забезпечення громадського порядку в зоні надзвичайної ситуації;

– проведення першочергового ремонту та відновлення роботи пошкоджених об’єктів життєзабезпечення населення, транспорту і зв’язку;

– здійснення заходів соціального захисту постраждалих внаслідок надзвичайних ситуацій;

– проведення інших робіт та заходів залежно від характеру та виду надзвичайної ситуації.

2. Авіаційний пошук і рятування постраждалих внаслідок аварії (катастрофи) повітряного судна здійснюється суб’єктами забезпечення цивільного захисту відповідно до компетенції. Організація пошуку та рятування таких постраждалих покладається на центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту.

3. Аварійно-рятувальні та інші невідкладні роботи проводяться відповідно до порядку, що визначається інструкціями, правилами, статутами, іншими нормативними документами щодо дій у надзвичайних ситуаціях, які затверджуються відповідними центральними органами виконавчої влади.

4. Аварійно-рятувальні та інші невідкладні роботи, гасіння пожеж проводяться в максимально стислі строки, безперервно до їх повного завершення, з найбільш повним використанням можливостей сил і засобів, неухильним дотриманням вимог встановлених режимів робіт та правил безпеки.

5. В окремих випадках з урахуванням вимог статті 103 Кодексу цивільного захисту України для ліквідації наслідків надзвичайних ситуацій можуть залучатися особи, які навчаються у навчальних закладах цивільного захисту.

6. Транспортні засоби аварійно-рятувальних служб, які мають кольоровографічні позначення встановленого зразка, спеціальні звукові та світлові сигнали, під час прямування до зони надзвичайної ситуації мають право безперешкодного проїзду, позачергового придбання пального та мастильних матеріалів.

7. Пересування автомобільними дорогами великогабаритних та великовагових транспортних засобів до місця проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій та у зворотному напрямку здійснюється на підставі дозволу відповідного підрозділу Міністерства внутрішніх справ України, що видається невідкладно, протягом однієї години, згідно з поданою заявкою, без проведення додаткових процедур погодження.

Для проведення АРІНР використовують всі сили ЦЗ, які є в розпорядженні начальників ЦЗ. Безпосередньо до сил ЦЗ належать: оперативно-рятувальна служба цивільного захисту; аварійно-рятувальні служби; формування цивільного захисту; спеціалізовані служби цивільного захисту; пожежно-рятувальні підрозділи (частини); добровольні формування цивільного захисту, а також організації та установи, що притягаються для вирішення завдань ЦЗ.

Зміст невідкладних аварійно-відбудовних робіт. Прокладка колонних шляхів та улаштування проїздів у завалах і на заражених ділянках; локалізація аварій на газових, енергетичних та інших мережах; зміцнення або обвалення конструкцій будинків і споруд, що загрожують обвалом, які перешкоджають безпечному руху і проведенню рятувальних робіт; відновлення і ремонт ушкоджених захисних споруд.

АРІНР організують у мінімально короткий термін і проводять безупинно вдень і вночі, у будь-яку погоду, до повного їх завершення. Це вимагає від начальника ЦЗ, штабу, служб і формувань високої організованості, а від особового складу – високої морально-психологічної стійкості, фізичної витривалості і мобілізації всіх сил.

Успішне проведення рятувальних і невідкладних аварійно-відбудовних робіт досягається: своєчасною організацією і безупинним веденням розвідки; створенням угруповання сил і засобів, швидким їхнім висуванням на ділянку (об'єкт) робіт; морально-психологічною підготовкою особового складу органів керування і формувань; активною участю населення в проведенні рятувальних робіт і умінням надавати першу медичну допомогу ураженим; умілою допомогою з боку начальників штабів і служб ЦЗ, діяльністю підлеглих при організації і проведенні АРІНР, організацією і підтримкою безупинної взаємодії органів керування, формувань , інших сил та засобів, залучених до рятувальних і невідкладних аварійно-відбудовних робіт.

Угруповання сил і засобів ЦЗ для організованого проведення АРІНР створюються в мирний час рішенням начальника ЦЗ району. Склад і побудова угруповання уточнюються при загрозі надзвичайної ситуації, а також після нанесення ядерних ударів відповідно до сформованої обстановки, наявності і стану збережених сил і засобів, обсягу робіт в осередках ураження.

В угруповання сил включаються об'єктні і територіальні формування міських і сільських районів, а також військові частини ЦЗ. Вони можуть складатися з формувань першого, другого ешелонів і резерву. Формування, що входять до складу ешелонів, розподіляються по змінам з дотриманням цілісності їх організаційної структури і виробничого принципу. Склад ешелонів, кількість і склад змін визначаються виходячи з конкретної обстановки, що склалася в осередках ураження, а також при наявності сил і засобів.

У період приведення ЦЗ в готовність начальник, штаб і служби ЦЗ об'єкта проводять заходи, передбачені планом. За розпорядженням старшого

начальника організовується вивід формувань за міську зону, у заздалегідь установлені райони розташування. У заміській зоні формування розташовуються в населених пунктах, на місцевості, що має природні укриття. У районі розташування зберігаються організаційна структура і цілісність формувань; забезпечується надійний захист особового складу і техніки від впливу зброї масового ураження, зручність розміщення і відпочинку, сприятливі санітарно-епідемічні умови. Створюються умови для швидкого збору формувань, підготовляються шляхи для висування формувань до об'єктів робіт. У районі розташування організується спостереження за зараженістю зовнішнього середовища і всебічне забезпечення.

Формування, які виділені рішенням старшого начальника, прискорено будують протирадіаційні укриття для населення і пристосовують придатні для цих цілей споруди.

Якщо формування розташовуються в населеному пункті, то на передбачуваному напрямку висування до осередку ураження призначається район збору формувань.

Формування можуть висуватися в складі загальної колони сил ЦЗ району чи самостійно. У першому випадку порядок висування визначається начальником ЦЗ району, у другому – начальником цивільного захисту об'єкта. До початку висування формування виводяться в район збору, що призначається завчасно в безпосередній близькості від маршруту руху.

Штаб і служби ЦЗ об'єкта організують керування підлеглими і взаємодіючими формуваннями, аналізують отримані дані про обстановку, роблять розрахунки можливого обсягу аварійно – рятувальних і невідкладних робіт та визначають необхідну кількість сил і засобів для їхнього виконання. Вчасно доводять усі розпорядження і задачі до формувань, надають необхідну допомогу і здійснюють контроль за їх виконанням, інформують вищий штаб про обстановку, що склалася, і її зміни, а також про дії сил об'єкта.

Завдання формуванню щодо проведення аварійно – рятувальних та інших невідкладних робіт ставить начальник ЦЗ об'єкта. Командир

формування, одержавши таку задачу, після її з'ясування й ухвалення рішення ставить задачі підлеглим, віддає необхідні розпорядження і організовує висування формування в осередок ураження.

Формування об'єкта для висування в осередок ураження шикуються в похідну колону. Порядок побудови колони встановлюється залежно від сформованої обстановки на маршрутах руху і ділянках (об'єктах) робіт. Один з можливих варіантів побудови колони: розвідка, загін забезпечення руху (ЗЗР), колона головних сил (перший та другий ешелони), резерви, технічне забезпечення.

Командир формування особисто керує висуванням формування. Він перевіряє готовність його до руху і віддає розпорядження про початок висування. У ході висування командир формування знаходиться в голові колони. За допомогою радіо і сигнальних засобів він підтримує постійний зв'язок, здійснює керування формуваннями і доданими засобами, підтримує встановлений порядок і заходи безпеки, стежить за дотриманням установленої швидкості руху, своєчасним проходженням вихідного пункту і пунктів регулювання. У випадку змін обстановки на маршруті негайно доповідає штабу, начальнику ЦЗ й інформує формування і сусідів.

У першу чергу задачі ставляться розвідці і формуванням, що входять до складу ЗЗР. Розвідці вказується, які дані і до якого часу добути, а загону забезпечення руху – склад, маршрут руху, час проходження вихідного рубежу (пункту), задачі по забезпеченню висування сил і засобів, обсягів робіт, порядок дії після виконання задачі. До складу ЗЗР (такий загон один на кожний маршрут) входять формування загального призначення, посилені формуваннями служб.

Рухаючись по зазначеному маршруту, загін на підставі даних розвідки відновлює зруйновані ділянки доріг, прокладає колоні шляхи в обхід завалів, руйнувань, пожеж, зон з високими рівнями радіації; відновлює й обладнує переправи; улаштовує проїзди в завалах; локалізує і гасить пожежі; укріплює або руйнує конструкції будинків, що загрожують обвалом. Головні зусилля ЗЗР

зосереджує на забезпеченні своєчасного висування сил ЦЗ до осередку ураження і швидкого введення їх на об’єкт робіт.

За загоном забезпечення руху висуваються головні сили ЦЗ об’єкта. На чолі колони звичайно їде начальник ЦЗ об’єкта, його штаб і начальники служб. Вони приймають усі заходи для того, щоб формування об’єкта в стані повної готовності до проведення АРІНР і в установлений час вийшли до осередку ураження. Начальник ЦЗ на підставі аналізу отриманих даних і сформованої обстановки на маршруті руху віддає необхідні розпорядження про подолання (обхід) зон зараження, зруйнованих ділянок маршруту, переправ, ділянок завалів і пожеж. Командири формувань забезпечують своєчасний вихід формувань до осередку ураження й організовують введення їх на об’єкти робіт.

6.2.2 Захист інформаційних управляючих систем від ушкоджень, що викликані дією ЕМІ ядерних вибухів

Електромагнітний імпульс виникає під час потужного вибуху (переважно атомної бомби), явищ, що викликають раптові збурення магнітного поля Землі, грозових явищ у земній атмосфері чи короткого замикання в електрообладнанні високої потужності.

Електромагнітний імпульс, який виникає під час ядерного вибуху більшість своєї енергії переносить в електромагнітних хвилях з частотою в діапазоні від 3 Гц до 30 кГц за напруженості магнітного поля, що досягає 50000 В/м [66].

Переважно розглядають два види електромагнітних імпульсів:

– ядерний ЕМІ (англ. Nuclear Electromagnetic Pulse, NEMP) – імпульс, що виникає під час ядерного вибуху;

– ЕМІ від розряду блискавки (англ. Lightning Electromagnetic Pulse, LEMP) – імпульс, що виникає під час електричного розряду в атмосфері.

Електромагнітний імпульс індукує високу електричну напругу в електромережах, електричному і електронному обладнанні. Зростання напруженості спричиняє раптове зростання електричної напруги і виділення

великої кількості тепла, внаслідок чого зазнають пошкоджень електронні елементи, електричні кола і навіть лінії електропередачі. Високі напруги також можуть призвести до пробою електричної ізоляції.

Зміна властивостей іоносфери Землі, викликана ЕМІ призводить до появи завад у радіозв'язку [66].

Уражаюча дія ЕМІ обумовлена виникненням напруг і струмів в провідниках різної довжини, розташованих в повітрі, на землі, в техніці, спорудах та інших об'єктах.

Основною причиною генерації ЕМІ тривалістю менше 1 с, вважають взаємодію γ-квантів і нейтронів з газом у фронті ударної хвилі і навкруги неї.

При наземному і низькому повітряному вибуху вражаюча дія ЕМІ спостерігається на відстані порядку декількох кілометрів від центру вибуху.

При висотному ядерному вибуху (Н > 10 км) можуть виникати поля ЕМІ в зоні вибуху і на висоті 20-40 км від поверхні землі [67].

Електричні та магнітні поля ЕМІ в ролі вражаючого фактора характеризуються напруженістю поля. В динаміці імпульс ЕМІ являє собою швидко затухаючий коливальний процес з кількома квазінапівперіодами. Напруженість електричного і магнітного полів залежить від потужності, висоти вибуху, відстані від центру вибуху і властивостей навколишнього середовища.

Уражаюча дія ЕМІ проявляється перш за все по відношенню до інформаційних управляючих систем, яка знаходиться на озброєнні, військовій і цивільній техніці та інших об'єктах. Під дією ЕМІ в зазначеній апаратурі наводяться електричні струми і напруги, які можуть викликати пробій ізоляції, ушкодження трансформаторів, згорання розрядників, псування напівпровідникових приладів, перегорання плавких вставок та інших елементів радіотехнічних пристроїв. Найбільш піддані впливу ЕМІ лінії зв'язку, сигналізації і управління. Якщо ЕМІ недостатні для повного пошкодження приладів або окремих деталей, то можливо спрацьовування засобів захисту (плавких вставок) і порушення працездатності ліній [67].

Електромагнітний імпульс являє небезпеку і для міцних споруд (укритих командних пунктів, ракетних стартових комплексів, об'єктів економіки), які розраховані на стійкість до впливу ударних хвиль наземного ядерного вибуху, проведеного на відстані кількох сотень метрів. У цьому випадку сильні електромагнітні поля можуть пошкодити електричні ланцюги і порушити роботу неекранованого електронного і електротехнічного обладнання.

Висотний вибух здатний створювати перешкоди в роботі засобів зв'язку на дуже великих площах.

Захист від ЕМІ досягається екрануванням каналів енергопостачання та управління, а також апаратури. Всі зовнішні лінії повинні бути двухпровідними, добре ізольованими від землі, з малоінерційними розрядниками і плавкими вставками. Для захисту чутливого електронного обладнання доцільно використовувати розрядники з невеликим порогом спалювання. Важливе значення мають правильна експлуатація ліній, контроль справності засобів захисту, а також організація обслуговування ліній в процесі експлуатації [67].

7 ЕКОЛОГІЯ

7.1 Аналіз сучасних програмних продуктів для опрацювання великих масивів екологічної інформації

Оперативна, якісна і точна обробка великих масивів статистичної інформації може бути виконана лише з використанням сучасних засобів обчислювальної техніки. Наявність потужних, надійних і разом з тим простих в експлуатації програмних продуктів статистичного аналізу звільняє дослідника від рутинних операцій, розширює сферу застосування статистичних методів в різних галузях людської діяльності, сприяє появі якісно нових можливостей статистичного аналізу і моделювання даних. Використання пакетів прикладних програм - це єдиний реальний практичний інструмент розв'язування задач багатофакторного кореляційно-регресійного та аналізу в багатовимірному просторі.

Програмне забезпечення статистичних досліджень досить розвинуте. Сучасний ринок програмних продуктів пропонує різноманітні пакети програм для статистичної обробки даних. Всесвітньо відомі статистичні пакети для комплексної обробки даних: *BMDP, SPSS, SAS, Systat, Minitab, S-Plus, Statgraphics Statistica* та інші.

Використання згаданих пакетів програм дає змогу автоматизувати процес статистичного дослідження в таких напрямах: створення файлів даних і таблиць; групування даних; графічний аналіз даних; розрахунок варіаційних характеристик вибіркових сукупностей; побудова рядів розподілу; аналіз рядів динаміки і прогнозування їх майбутніх рівнів; кореляційно-регресійний аналіз; багатомірний аналіз.

З 1995 р. Світовим лідером на ринку статистичного програмного

забезпечення визнається інтегрована система *Statistica* для *Windows* (версія 5.0), розроблена фірмою Stat Soft. Перша версія програми з'явилася у 1991 р. для операційної системи MS-DOS і була новим напрямом розвитку статистичного програмного забезпечення. В ній реалізовано графічно-орієнтований підхід до статистичного аналізу даних, суть якого полягає в отриманні всебічного візуального представлення інформації на всіх етапах статистичної обробки даних.

Багатофункціональна, графічно орієнтована на обробку масових даних система *Statistica* відповідає основним стандартам *Windows* (динамічний обмін даними з іншими додатками, підтримка основних операцій з буфером обміну, робота в мережевому середовищі та інші).

Передусім це стандарти користувацького інтерфейсу — *MDI,* використання буфера-обміну, механізму динамічного зв'язку *(DDE)* з іншими додатками; система підтримує всі операції, реалізовані за допомогою методу *Drag-and-Drop* — «Перетягти та опустити», включаючи автозаповнення, інші.

Складніші процедури обробки даних у системі *Stratgraphics* виконує спеціалізований модуль *Data Management* — «Управління даними», а для обробки великих масивів даних або даних з довгими текстовими значеннями застосовують процедури *Megafile Manager Data* — «Менеджера мегафайлів».

Система *Stratgraphics* працює з чотирма типами документів. Це:

– *електронна* таблиця *Spreadsheet,* призначена для введення і перетворення первинних даних;

– *електронна* таблиця *Scrollsheet* — для виведення результатів аналізу;

– *графік* — для візуалізації результатів обробки та аналізу даних;

– *звіт* — файл у формі *RTF* (розширений текстовий формат), в якому зберігається текстова, числова і графічна інформація.

Усі статистичні процедури системи розбито на окремі модулі, кожен з яких об'єднує групу логічно зв'язаних між собою статистичних методів і в рамках конкретної моделі забезпечує повний і всебічний аналіз

закономірностей.

Модуль *Multiple Regression* — «Множинна регресія» включає: вичерпний набір засобів множинної лінійної і нелінійної регресії, багатофакторного прогнозування, аналіз залишків і викидів, тестування гіпотез регресійного аналізу.

Модуль *Time Series/Foreca*sting — «Часові ряди і прогнозування» об'єднує процедури аналізу закономірностей динаміки: тенденцій розвитку і коливань, різні методи згладжування рядів, описування трендів, описування сезонної декомпозиції, методи авторегрсійного аналізу, методи прогнозної екстраполяції.

Система Statistica включає модуль Anova/Manova — «Дисперсійний аналіз», увесь арсенал методів багатовимірного аналізу (кластерний, дискримінантний, факторний аналіз, факторне шкалювання, канонічні кореляції).

Особливе місце посідає модуль Sepath — «Моделювання взаємозв'язків системами структурних рівнянь».

Зазначені модулі покривають практично весь спектр сучасних методів статистичного дослідження і моделювання. Запуск модуля здійснюється через перемикач модулів — Module Swither. У кожному модулі робота починається із «Стартової панелі», де відкривається файл первинних даних, вибирається процедура обробки даних і визначаються відповідні їй параметри.

Стартова панель — основне діалогове вікно модуля. Структуру діалогу в усіх модулях уніфіковано, її можна подати схематично (див. рисунок 7.1).

У системі *Statistica* реалізовано принцип постійного логічного підказування. Якщо користувач не може визначитися щодо наступного кроку діалогу, через команду *Enter* система сама спрямує до відповідного діалогового вікна. Якщо виникають складнощі з вибором параметрів обчислювальної процедури, вони задаються системою «за умовчуванням».

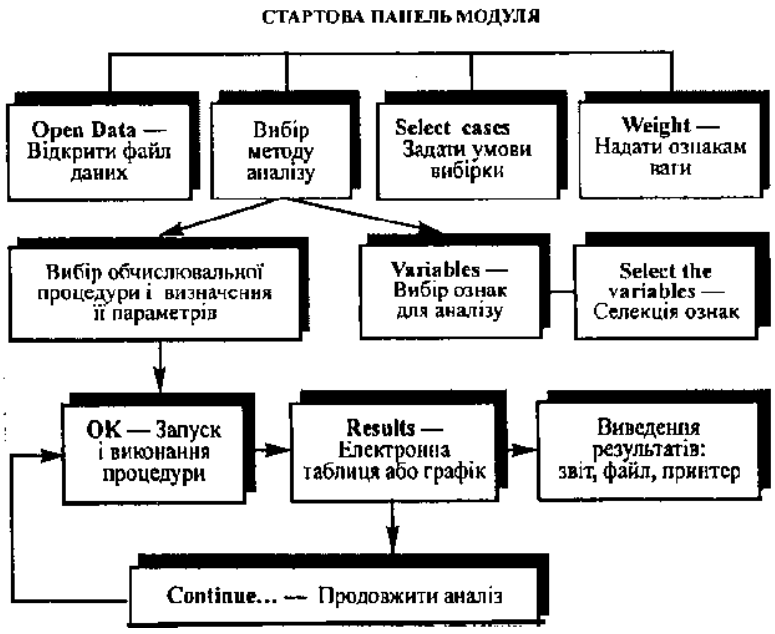

Рисунок 7.1 – Схема структури діалогу в модулі

Важливою характеристикою системи є наявність засобів всебічної графічної підтримки процесу обробки даних і візуалізації результатів аналізу. Графічні можливості й засоби системи унікальні. Вона включає сотні різних типів користувацьких і спеціальних статистичних графіків, доступних у будь-якому модулі й на будь-якому етапі статистичної обробки даних. Інструменти компонування складної графічної інформації з текстовою і числовою інформацією розглядаються у кожному модулі.

Використання сучасних комп'ютерних технологій обробки даних, інтерактивний спосіб взаємодії з системою перетворюють статистичний аналіз, моделювання та прогнозування в захоплююче дослідження закономірностей навколишнього світу. Завдяки різноманітним формам організації діалогу, максимально простій із звичними для статистики термінами мові спілкування, наявності контекстно-залежної довідкової системи, мові програмування STATISTICA BASIC пакет є ефективним інструментом проведення статистичного дослідження як для користувача-початківця, так і для професіонала.

7.2 Кореляційний аналіз зв’язків в екології

Кореляцією називається неповний зв'язок між досліджуваними явищами. Це така залежність, коли будь-якому значенню однієї змінної величини може відповідати декілька різноманітних значень іншої змінної. Вона відображає закон множини причин і наслідків і є вільною неповною залежністю. Кореляція – взаємозв'язок між ознаками, що полягає в зміні середнього значення однієї з них залежно від зміни іншої. Ознаки, пов'язані кореляційним зв'язком, називаються корельованими.

Кореляційний аналіз – метод, що вивчає кількісні характеристики кореляційних зв’язків.

Кореляційний аналіз є свого роду логічним продовженням (розвитком) методу статистичних групувань, його поглибленням. Він допомагає вирішити цілий ряд нових завдань в економічному аналізі. Розрахунки на основі кореляційних моделей підвищують ступінь точності аналізу, часто виявляють недоліки попереднього аналізу. Перевага цього методу полягає також і в тому, що він дає можливість розв'язувати задачі, які не можна вирішити за допомогою інших методів економічного аналізу, як, наприклад, відокремлення впливу багатьох факторів, які діють взаємопов'язано і взаємозумовлене. У дослідженнях важливо вивчати не стільки міру кореляції, скільки форму її й характер зміни однієї ознаки залежно від зміни іншої. Ці задачі розв'язуються методами регресійного аналізу.

Використання методу кореляції і регресії дозволяє вирішити такі основні завдання:

– встановити характер і тісноту зв'язку між досліджуваними явищами;

– визначити і кількісно виміряти ступінь впливу окремих факторів і їх комплексу на рівень досліджуваного явища;

– на підставі фактичних даних моделі залежності екологічних показників від різних факторів розраховувати кількісні зміни аналізованого

явища при прогнозуванні показників і давати об'єктивну оцінку діяльності підприємств.

Суть кореляційного аналізу полягає в побудові, рішенні й аналізі економіко-математичної моделі у виді функції (рівняння) зв'язку між результативною та факторною або факторними ознаками.

Статистичне дослідження кореляційної залежності включає завдання визначення форми зв'язку і знаходження кількісної характеристики цієї форми. Процес встановлення форми зв'язку і вибору математичного рівняння, яке могло б найбільш повно відображати характер взаємозв'язку між ознаками досліджуваного явища, має вирішальне значення в кореляційному аналізі. Важливість цього етапу полягає в тому, що правильно встановлена форма зв'язку дає змогу добрати й побудувати найбільш адекватну модель і на основі її розв'язання отримати статистично достовірні й надійні характеристики зв'язку.

Під формою кореляційного зв'язку розуміємо тип аналітичного рівняння, що виражає залежність між досліджуваними ознаками.

Розрізняють дві форми зв'язку: лінійну і нелінійну. Лінійна виражається рівнянням прямої лінії, нелінійна — рівнянням кривих ліній: гіперболи, параболи, степеневої, показникової тощо. За напрямами зв'язки бувають прямими й зворотними. В першому випадку обидві ознаки змінюються в одному напрямі, тобто із зростанням факторної ознаки зростає результативна і навпаки, а в другому випадку обидві ознаки змінюються в різних напрямах. За щільністю зв'язки бувають – сильними, слабкими та ін. Коли визначається зв'язок між двома ознаками, кореляція називається простою; якщо ж явище розглядається як результат впливу декількох факторів – множинною.

Встановлення форми зв'язку означає вибір рівняння регресії, що найбільш повно відбиває характер взаємодії між результатом і фактором, за яким проводитимуться розрахунки.

Особливості, властиві кореляційному аналізу:

– при використанні кореляційного методу вирішальне значення має всебічний, економічно усвідомлений попередній аналіз даних господарської діяльності. Слід пам'ятати, що зв'язок між ознаками і властивостями – не результат математичних розрахунків, а лежить у природі самих екологічних явищ і за допомогою методів математичної статистики можна лише об'єктивно виразити існуючі закономірності економічних процесів;

– кореляцію можна виявити, лише досліджуючи достатньо велику сукупність спостережень, оскільки кореляційні зв'язки виявляються у формі спряженого варіювання двох або кількох зіставлених ознак.

Кореляційно-регресійний аналіз включає три етапи:

1) математико-екологічне моделювання;

2) рішення прийнятої моделі шляхом знаходження параметрів кореляційного рівняння (рівнянням регресії);

3) оцінка та аналіз одержаних результатів.

Значення кореляційного аналізу у тому, що параметри рівняння використовуються: як знаряддя цілеспрямованої зміни результатів, як знаряддя техніко-економічне нормування, планування, прогнозування, як критерії напруженості плану, як знаряддя впливу на кінцевий результат.

Вивчення взаємозв'язків кореляційного типу має істотне значення особливо при аналізі явищ, які складаються під впливом великої кількості певних умов.

7.3 Висновки до сьомого розділу

В розділі проведено аналіз сучасних програмних продуктів для опрацювання великих масивів екологічної інформації та розглянуто кореляційний аналіз зв’язків в екології.

ВИСНОВКИ

В результаті проведених досліджень можна зробити наступні висновки.

Загрози комп'ютерної безпеки діляться на явні і приховані. Під явними розуміємо такі погрози, які зрозумілі і однозначно передбачені. Вони не вимагають для протидії їм будь-яких додаткових відомостей про статистику погроз і неочевидних припущень про можливі атаки зловмисника.

Критерії оцінки захисту комп'ютера встановлюють базові вимоги щодо контролю комп'ютерної безпеки вбудованої в обчислювальну систему, використовуються, щоб оцінювати, класифікувати та обирати комп'ютерні системи, які використовуються для обробки, зберігання та надання доступу до класифікованої інформації.

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

В першому розділі наведено вимоги до захисту комп’ютерної інформації, а зокрема: описано формалізовані вимоги до захисту і їх класифікація,наведено вимоги до захисту конфіденційної інформації, наведено вимоги до захисту секретної інформації, а також описано відмінності вимог і засадничих механізмів захисту від НСД. Також описано об’єкти загроз та їх класифікація. Описано функційну модель системи захисту та тсновні групи механізмів захисту і наведено рекомендації по окремим рівням функціональної моделі. Також описано критерії оцінки захисту комп'ютера і критерії оцінки інформаційної безпеки.

В другому розділі проведено аналіз серверів Sun Microsystems.

Проаналізовано конфігурацію і технічні параметри серверів і процесорів SPARC, а зокрема архітектуру RISC і процесори SPARC і UltraSPARC. Проведено аналіз категорії серверів: сервери початкового рівня, сервери середнього рівня, високопродуктивні сервери, блейд-сервери, сервери зберігання даних, кластери Sun та NEBS-сертифіковані сервери.

В третьому розділі проведено розробку методики вибору системи захисту інформації, а також проведено вибір методу системи захисту. Проведено аналіз і постановка задачі вибору системи захисту інформації . Описано використання системи захисту конфіденційної інформації PGP, а зокрема наведено основні характеристики системи PGP, проведено ініціалізацію системи PGP на робочій станції. Описано засоби протидії несанкціонованому доступу.

Розглянуто ряд додаткових розділів.

В розділі “Спеціальна частина” описано спосіб пошуку Malware.

В розділі “Обґрунтування економічної ефективності” проведено економічні розрахунки, спрямовані на визначення економічної ефективності від оптимізації системи захисту локальної мережі з використанням серверів Sun Microsystems, а також прийнято рішення щодо подальшого розвитку. Розраховано значення економічної ефективності становить 0,559, що є високим значенням. Так само нормальним є термін окупності. Для даного дослідження він становить 1.78 року.

В розділі “Охорона праці та безпека в надзвичайних ситуаціях” розглянуто психологію безпеки праці і ергономіку; характеристику вогнегасних речовин та підвищення стійкості роботи об'єктів господарської діяльності у воєнний час.

В розділі “Екологія” проведено аналіз сучасних програмних продуктів для опрацювання великих масивів екологічної інформації та розглянуто кореляційний аналіз зв’язків в екології.

ПЕРЕЛІК ПОСИЛАНЬ

1. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий [Текст] : РД: утв. Гостехкомиссией России. - М., 2002.

2. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию [Текст]. - Введ. 2000-01-01 - М.: Изд-во стандартов, 1999. - 8 с.

3. Гарасим Ю. Р. Концепція організації системи захисту інформації на відомчих цифрових системах комутації /Ю. Р. Гарасим, В. В. Хома // Зб. наук. статей «Управління розвитком» МНПК «Сучасні засоби та технології розроблення інформаційних систем». - Харків: ХНЕУ, 2008. - № 15. - С. 41-42.

4. Гарасим Ю. Р. Технології функціонування захищених корпоративних мереж зв'язку / Ю. Р. Гарасим // Современные информационные и электронные технологии : Мат. науч. трудов десятой МРПК. - Одесса, 2009. - С. 63.

5. Гарасим Ю. Р. Деякі аспекти інформаційної безпеки корпоративних мереж зв 'язку / Ю. Р. Гарасим // II тур Всеукраїнського конкурсу студентських наукових робіт з технічних наук, напрям «Телекомунікації», спеціальності «Телекомунікаційні системи та мережі», «Інформаційні мережі зв'язку» : Тез. доп. - Одеса, 2009. - С. 19.

6. ГарасимЮ.Р. Інформаційна безпека захищених корпоративних мереж зв'язку /Ю.Р.Гарасим, В.Б.Дудикевич // Вісник Національного університету «Львівська політехніка» «Автоматика, вимірювання та керування». - Львів, 2009. - № (639). - С. 124-132.

7. Гарасим Ю. Р. Структура технологій функціонування систем захисту інформації корпоративних мереж зв 'язку / Ю. Р. Гарасим,

8. Б. Дудикевич //Матеріали IVМНПК «Спеціальна техніка у правоохоронній діяльності». - К., 2009. - 226-228.

9. Гарасим Ю. Р. Поняття живучості системи захисту інформації захищених корпоративних мереж зв 'язку /Ю. Р. Гарасим, В. Б. Дудикевич //Тези доп. IIIМНПК «Інформаційна та економічна безпека (INFEC0-2010)». - Харків, 2010. - Вип. 3(84). - С. 107-109.

10. Гарасим Ю. Р. Живучість розподіленої системи управління системою захисту інформації в захищених корпоративних мережах зв 'язку та її моделі /Ю. Р. Гарасим, В. Б. Дудикевич //Труди ХІМНПК «Сучасні інформаційні та електронні технології». - Одеса, 2010. - Т.1. - С. 96.

11. Dudykevych V. Survivable security Systems Analysis / V. Dudykevych, I. Garasym //Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT, 2010. - Lviv: Publishing House Vezha&Co, 2010. - pp. 108-110.

12. Дудикевич В. Б. Системи захисту інформації, що мають властивість живучості. Основні поняття / В. Б. Дудикевич, Ю. Р. Гарасим // Науково-технічний журнал «Сучасний захист інформації», спеціальний випуск. - 2010. - № 4. - С. 6-13.

13. Гарасим Ю. Р. Модель захищеної корпоративної мережі зв 'язку, яка має властивість живучості / Ю. Р. Гарасим, В. Б. Дудикевич //Зб. тез VIМНТК «Сучасні інформаційно-комунікаційні технології». -АР Крим, Ялта-Лівадія, 2010. - С. 196-197.

14. Ларичев О. И. Теория и методы принятия решений /О. И. Ларичев. - М. : Логос, 2000. - 296с.

15. Катренко А. В. Теорія прийняття рішень /А. В. Катренко, В. В. Пасічник, В. П. Пасько. - К.: Видавнича група BHV, 2009. - 448с.

16. Черкесов Г. Н. Методы и модели оценки живучести сложных систем /Г. Н. Черкесов. -М., 1987. - 38с.

17. Гиг Дж. Прикладная общая теория систем: пер. с англ. / Дж. ванГиг. -М.:Мир, 1981. - 336с.

18. Гайдес М. А. Общая теория систем. (Системы и системный анализ) / М. А. Гайдес. - Глобус-пресс, 2005. - 202с.

19. Цофнас А. Ю. Теория систем и теория познания / А. Ю. Цофнас. - Одесса : АстроПринт, 1999. - 308с.

20. Згуровський М. З. Основи системного аналізу /М. З. Згуровський, Н. Д. Панкратова. - К.: Видавнича група BHV, 2007. - 544с.

21. Верлань А. Ф., Сизиков В. С. Интегральные уравнения: методы, алгоритмы, программы. — К.: Наук. думка, 1986. — 544 с.

22. Манжиров А. В, Полянин А. Д. Справочник по интегральным уравнениям. Методы решения. — М.: Физматлит, 2003. — 608 с.

23. Тихонов А. Н, Арсенин В. Я. Методы решения некорректных задач. — М.: Наука, 1986. — 288 с.

24. Катренко А. В. Теорія прийняття рішень /А. В. Катренко, В. В. Пасічник, В. П. Пасько. - К. : Видавнича група BHV, 2009. - 448с.

25. Петров Э. Г. Методы и средства принятия решений в социально-экономических и технических системах / Э. Г. Петров, М. В. Новожилова, И. В. Гребенник, Н. А. Соколова. - Херсон: ОЛДІ-плюс, 2003. - 380 с.

26. Литвак Б. Г. Экспертные оценки и принятие решений /Б. Г. Литвак. -М.: Патент, 1996. - 271 с.

27. Тинякова В. И. Математические методы обработки экспертной информации /В. И. Тинякова. - Воронеж, 2006. - 68с

28. ГОСТ Р 50922-96. Защита информации. Основные термины и определения [Текст]. М.: Изд-во стандартов, 1996.

29. ГОСТ Р 51624-2000. [Текст]. М.: Изд-во стандартов, 2000.

30. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации [Текст] : РД : утв. Гостехкомиссией России. - М.: Изд-во стандартов, 1992.

31. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации [Текст] : РД : утв. Гостехкомиссией России. - М.: Изд-во стандартов, 1992.

32. Защита от несанкционированного доступа к информации. Термины и определения [Текст] : РД : утв. Гостехкомиссией России. - М.: Изд-во стандартов, 1992.

33. ГОСТ Р 15408-02. Критерии оценки безопасности информационных технологий [Текст]. - Введ. 2004-01-01 - М.: Изд-во стандартов, 2002.

34. ISO/IEC 17799:2000. Информационные технологии. Свод правил по управлению защитой информации. Международный стандарт [Текст] / ISO/IEC, 2000.

35. Зегжда Д. П. Как построить защищенную информационную систему. Технология создания безопасных систем [Текст] / Д. П. Зегжда, А. М. Ивашко ; под научн. ред. П. Д. Зегжды, В. В. Платонова. - СПб.: Мир и Семья-95, Интерлайн, 1998. - 256 с. : ил. ; 20 см. - 500 экз.

36. Девянин П. Н. Теоретические основы компьютерной безопасности [Текст]: учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. - М.: Радио и связь, 2000. - 192 с. : ил. ; 21 см.

37. Ресурсы Microsoft Windows NT Workstation 4.0 [Текст] : [пер. с англ.] / Корпорация Майкорософт. - СПб. : BHV - Санкт-Петербург, 1998. - 800 с. : ил. ; 28 см. + 1 электрон. опт. диск. - Перевод изд.: Microsoft Windows NT Workstation 4.0 Resource Kit / Microsoft Corporation, 1996.

38. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах [Текст]: учеб. пособие для вузов / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. - М.: Радио и связь, 2000. - 168 с. : ил.

39. Гайдамакин Н. А. Автоматизированные системы, базы и банки данных. Вводный курс [Текст]: учеб. пособие / Н. А. Гайдамакин. - М.: Гелиос АРВ, 2002. - 368 с. : ил.

40. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. - Екатеринбург: Изд-во Урал. Ун-та, 2003. - 328 с. : ил.

41. Хорев П. Б. Методы и средства защиты информации в компьютерных системах [Текст]: учеб. пособие для вузов / П. Б. Хорев. - М.: Академия, 2005. - 256 с. : ил.

42. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А. Ю. Щеглов ; под ред. М. В. Финкова. - СПб: Наука и Техника, 2004. - 384 с. : ил.

43. Система защиты информации от несанкционированного доступа «СТРАЖ NT». Версия 2.0. Описание применения. УИМ.00025-01 31 [Электронный ресурс]. - 53 с. : ил.

44. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0». Руководство по эксплуатации [Электронный ресурс]. - 88 с. : ил.

45. Система защиты информации «Secret Net 2000. Автономный вариант для Windows 2000». Руководство по администрированию [Электронный ресурс]. - 142 с. : ил.

46. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-NT/2000» (версия 2.0). Описание применения [Электронный ресурс]. - 30 с. : ил.

47. Система защиты конфиденциальной информации StrongDiskPro. Версия 2.8.5. Руководство пользователя [Электронный ресурс]. - 31 с. : ил.

48. Система защиты конфиденциальной информации Secret Disk. Версия 2.0. Руководство пользователя [Электронный ресурс]. - 116 с. : ил.

49. Петров А. А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А. А. Петров - М.: ДМК, 2000. - 448 с. : ил.

50. Молдовян А. А. Криптография [Текст] / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. СПб.: Лань, 2000. - 224 с. : ил.

51. Алферов А. П. Основы криптографии [Текст]: учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. - М.: Гелиос АРВ, 2001. - 480 с. : ил.

52. Брассар Ж. Современная криптология. Руководство [Текст] : [пер. с англ.] / Ж. Брассар. - М.: ПОЛИМЕД, 1999. - 176 с. : ил.

53. Разработка политики безопасности организации в свете новейшей нормативной базы / А. С. Марков, С. В. Миронов, В. Л. Цирлов // Защита информации. Конфидент. - 2004. - № 2 - С. 20-28.

54. Синадский Н. И. Угрозы безопасности компьютерной информации [Текст]: учеб. пособие / Н. И. Синадский, О. Н. Соболев - Екатеринбург: Изд-во Урал. ун-та, 2000. - 85 с.: ил.

55. Запечников, С.В. Основы построения виртуальных частных сетей [Текст]: Учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. — М.: Горячая линия-Телеком, 2003. — 249 с. ; 20 см. — 3000 экз. — ISBN 5-93517-139-2

56. http://www.oracle.com/webfolder/technetwork/hcl/index.html. Oracle Solaris OS: Hardware Compatibility Lists. (10.08.2016).

57. http://uk.wikipedia.org/wiki/Критерії_оцінки_захисту_комп'ютера. Критерії оцінки захисту комп'ютера. (11.08.2016).

58. http://uk.wikipedia.org/wiki/Критерії_інформаційної_безпеки. Common Criteria. (11.08.2016).

59. Жидецький В. Ц. Основи охорони праці: Підручник. / В.Ц. Жидецький - 4-те вид., перероб. і доп. - К.: Знання, 2010. - 375 с. + компакт-диск. – ISBN 978-966-346-601-9.

60. Запорожець О. І. Основи охорони праці. Підручник / О. І. Запорожець, О. С. Протоєрейський, Г. М. Франчук, І. М. Боровик – К.: Центр учбової літератури, 2009. – 264 с. – ISBN 978-966-364-934-4.

61. Цапко В.Г. Безпека життєдіяльності: Навч. посіб. / За ред. В.Г. Цапка. - 3-тє вид., стер. - К.: Знання, 2004. - 397 с. – ISBN 966-8148-39-8.

62. Завдання та функції служби охорони праці на підприємстві [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: http://oppb.com.ua/news/zavdannya-ta-funkciyi-sluzhby-ohorony-praci-na-pidpryyemstvi

63. Служба охорони праці: завдання, функції, документація [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://ohrana-truda.kiev.ua/ua/служба-охраны-труда-задачи-функции-до/

64. «20 самых востребованных профессий в Украине» – [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: http://changeua.com/business/20-samyih-vostrebovannyihprofessiy-v-ukraine/

65. Гігієнічні вимоги до організації і обладнання робочих місць користувачів комп'ютерів [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://cpo.stu.cn.ua/Oksana/posibnik/1010.html

66. Електромагнітний імпульс – [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://uk.wikipedia.org/wiki/електромагнітний_імпульс

67. Ядерна зброя і захист від неї – [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://studme.com.ua/11151212/bzhd/yadernoe_oruzhie_zaschita_nego.htm

68. Методичні вказівки до виконання дипломної роботи ОКР "Магістр" для студентів спеціальності 8.05010101– Інформаційні управляючі системи та технології / Укладачі: О. В. Маєвський, О.В. Мацюк, М.В. Приймак, Г.В. Шимчук – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2014. – 196 с.