МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОТФК ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна графіка і Web-дизайн»

Група: 4КГ-05

Дипломний проект

здобувача освіти денної форми навчання
КГ.05.08.000.ДП

Дубіненко Лідії Сергіївни

м. Одеса
2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Комп'ютерна графіка і Web-дизайн»**

Група: **4КГ-05**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка комплексних заходів безпеки інформаційних систем студії Web-дизайну

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на 14 аркушах (слайдах).

Дипломник _____ (Дубіненко Л.С)

Керівник _____ (Шевцов Ю.С.)

Консультанти:

з економічної частини _____ (Копайгородська Т.Г.)

з охорони праці_____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Скорнякова О.В.)

До захисту допущений

Голова циклової комісії _____ (Скорнякова О.В.)

Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»_____ 2022 р. Протокол ДКК №_____

Оцінка ДКК _____

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Комп'ютерна графіка і Web-дизайн»**

ЗАТВЕРДЖУЮ:

Заст. дир. з

НВР_____

_____

"_____"_____2022 р.

ЗАВДАННЯ

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти **Дубіненко Лідії Сергіївни**

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): **Розробка комплексних заходів безпеки інформаційних систем студії Web-дизайну**

затверджена наказом по коледжу від "**30**" **січня** 202**1** р. № **306-А2-ОД**

2. Термін здачі закінченого проекту (роботи)

3. Вихідні данні до проекту (роботи): **Usability аудит. Adobe Photoshop. Adobe Illustrator. Adobe Indesing. Adobe After Effects. Файл robots.txt. Kali Linux. LAN (Local Area Network). WAN (Wide Area Network). Damn Vulnerable Web Application (DVWA). Утиліта Nmap. JavaScript.**

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

ВСТУП.

1. **ТЕХНОЛОГІЧНИЙ РОЗДІЛ**
2. **ЕКОНОМІЧНИЙ РОЗДІЛ**
3. **ОХОРОНА ПРАЦІ**
4. **ВИСНОВКИ**

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Створення презентаційного матеріалу, кількість слайдів не менше 10

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Шевцов Ю.С.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання

_____

Керівник _____

(підпис)

Завдання прийняв до виконання _____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	Огляд літератури. Огляд існуючих рішень.		
2.	Формування кінцевого завдання на розробку. Вступна частина дипломного проекту.		
3.	Технологічний розділ. Інформаційні системи студії Web-дизайну		
4.	Технологічний розділ. Інформаційна безпека Web-дизайну		
5.	Технологічний розділ. Комплексна система захисту інформації студії Web-дизайну		
6.	Економічний розділ.		
7.	Виконання розділу «Охорона праці».		
8.	Підготовка доповіді та презентації для захисту		
9.	Підготовка до попереднього захисту, підготовка до захисту		
10.	Отримання рецензії, відповіді на зауваження рецензента		
11.	Захист роботи		

Дипломник _____

(підпис)

Керівник _____

(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КГ.05.08.000.ДП	Дипломний проект		
А4			КГ.05.08.000.ДП. ПЗ	Пояснювальна записка	1	
				Презентація	14	

Ізм.	Арк.	№ докум.	Підпис	Дата	КГ.05.08. 000.ДП		
Розробив		Дубіненко Л.С			Розробка комплексних заходів безпеки інформаційних систем студії Web-дизайну	Літ.	Аркуш	Аркушів
Перевірив		Шевцов Ю.С.				Н Д П		
Н. Контр.		Петрашова В.І.				ВСП ОТФК ОНТУ		
Затверд.		Скорнякова						

Зм.	Арк.	№ докум.	Підпис	Дата	ДП.КГ.05.08.00.00	Арк. 5

АНОТАЦІЯ

Мета даної роботи є розробка комплексних заходів безпеки інформаційних систем студії Web-дизайну. В даній випускній роботі молодшого спеціаліста розглянуто термінологічний фундамент, аналіз загроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в студії Web-дизайну з урахуванням сучасного стану і прогнозу розвитку методів, систем та засобів здійснення загроз зі сторони потенційних порушників. В рамках розробки комплексних систем захисту інформації студії Web-дизайну були досліджені:

1. Визначено основні поняття інформаційної безпеки студії Web-дизану.
2. Проведено аналіз ризиків інформаційних систем.
3. Побудували систему захисту інформацій
4. Визначено принпици КСЗ інформації в студії Web-дизайну.
5. Провели комплексну систему безпеки інформаційних систем студії Web-дизайну.

Зміст

ВСТУП

Сучасні інформаційно-комунікаційні системи та мережі уразливі до ряду загроз, які можуть бути результатом реалізації несанкціонованого доступу, розкриття, викривлення або модифікації інформації, а також обмеження доступу до неї. Ці уразливості мають тенденції до посилення. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи, засновані на комплексному підході до розробки та впровадження заходів та засобів захисту ресурсів інформаційно-комунікаційних систем та мереж як на технічному, так і на організаційному рівні. Зазначений процес забезпечує механізми та методи, які дозволяють реалізувати комплексну політику інформаційної безпеки організації. Інформаційна безпека – реалізація процесу захисту інформації від широкого діапазону загроз, що здійснюється з метою забезпечення ефективності та надійності функціонування інформаційно-ко Метою даного дипломного проекту є аналіз послуг і механізмів захисту інформацій систем студії Web-дизайну, а також особливостей їх реалізації на різних рівнях моделі взаємодії відкритих систем, розгляд основних концептуальних питань створення, функціонування, розвитку і використання національної системи конфіденційного зв'язку, вивчення основних загроз інформаційної безпеки комп’ютерних систем і мереж, а також протоколів та засобів захисту інформації в мережі Інтернет.

Інформаційна безпека студії Web-дизайну містить в собі заходи захисту процесів створення даних, їх введення, обробки і виведення. Метою інформаційної безпеки студії Web-дизайну є убезпечення цінності системи, захист і гарантування точності та цілісності інформації, мінімізація руйнування, що може мати місце, якщо інформація буде модифікована або зруйнована. Інформаційна безпека вимагає врахування всіх подій, в ході яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється.

1. Інформаційні системи студії Web-дизайну

Інформаційна система (ІС) - це сукупність засобів збору, зберігання, передачі, оброблення інформації для досягнення поставленої мети у процесі управління.

Автоматизована ІС - сукупність інформації, різних методів і моделей, апаратних, програмних, організаційних, технологічних засобів і відповідних фахівців. Отже, інформаційна система - це організаційно впорядкована сукупність фахівців, інформаційних ресурсів та інформаційних технологій, зокрема з використанням засобів обчислювальної техніки і зв'язку, що реалізовують такі інформаційні процеси, як отримання вхідних даних; обробка цих даних і/або зміна власного внутрішнього стану (внутрішніх зв'язків/відносин), видача результату або зміна свого зовнішнього стану (зовнішніх зв'язків/відносин). За допомогою ІС надається можливість встановлення зв'язку між усіма елементами бізнес-процесів підприємства, що покращує можливості планування, контролю й регулювання процесів.

Інформаційна система — система, призначена для зберігання, пошуку та обробки інформації, та відповідні організаційні ресурси (людські, технічні, тощо), які забезпечують та поширюють інформацію. Склад інформаційних систем:

- локальні мережі
- глобальні мережі
- комп'ютерні системи

ІС включає вхідну інформацію (дані, інструкції) та вихідну інформацію (звіти, розрахунки) і функціонує в інформаційному середовищі. За допомогою засобів обробки інформації вхідна інформація перетворюється на вихідну, і потім надсилається користувачу або іншій ІС. ІС може включати механізм зворотного зв'язку.

1.1. Структурна схема інформаційної системи

Засоби розробки та впровадження автоматизованих інформаційних систем включають технічне, програмне, інформаційне, організаційно-методичне, математичне, лінгвістичне, правове, технологічне забезпечення, що допомагають у їх створенні та експлуатації.

Базові види забезпечення ІС:

- о ***технічне*** - сукупність технічних засобів збору, передачі, введення, обробки, подання і виводу інформації; обладнання - комп'ютери і периферійні пристрої, носії інформації - дисководи (гнучкі дискети), вінчестери (жорсткі диски); пристрої читання лазерних дисків (CD-ROM), стримери й інші спеціальні пристрої, монітор, клавіатура, засоби організаційної техніки та допоміжного обладнання, мережа тощо;
- о ***програмне*** - сукупність програм загальносистемних (операційні системи), інструментальних (редактори, електронні таблиці), прикладних (спеціалізовані програмні застосування);
- о ***інформаційне*** - методи і засоби перетворення зовнішнього подання даних в машинні, опис інформації під час обробки, передачі інформації з машинного формату подання в зовнішній через машинне (база даних, база знань, сховище даних, СУБД, файли тощо) та немашинне

забезпечення (методики, що описують принципи роботи в ІС, системи класифікації та кодування, системи стандартизації документів тощо);

- о ***організаційно-методичне*** - сукупність організаційно-методичних засобів, що описують або реалізовують технологію проектування, функціонування і розвитку ІС для окремих її компонент і видів забезпечень, які охоплюють методи і засоби опису, формування, застосування певних організаційно-методичних процедур. Це організація роботи системи, що забезпечує управління підсистемами як єдиним цілим;
- о ***лінгвістичне*** - сукупність мов програмування, що працюють в ІС, мови управління і маніпулювання даними, мовні засоби пошукових систем, мовні засоби проектування ІС, діалогові мови;
- о ***математичне*** - сукупність засобів і методів, що дозволяють будувати математичні моделі задач управління та алгоритм їх рішення;
- о ***правове*** - сукупність норм, що представлені в нормативних документах, які встановлюють правовий статус ІС.

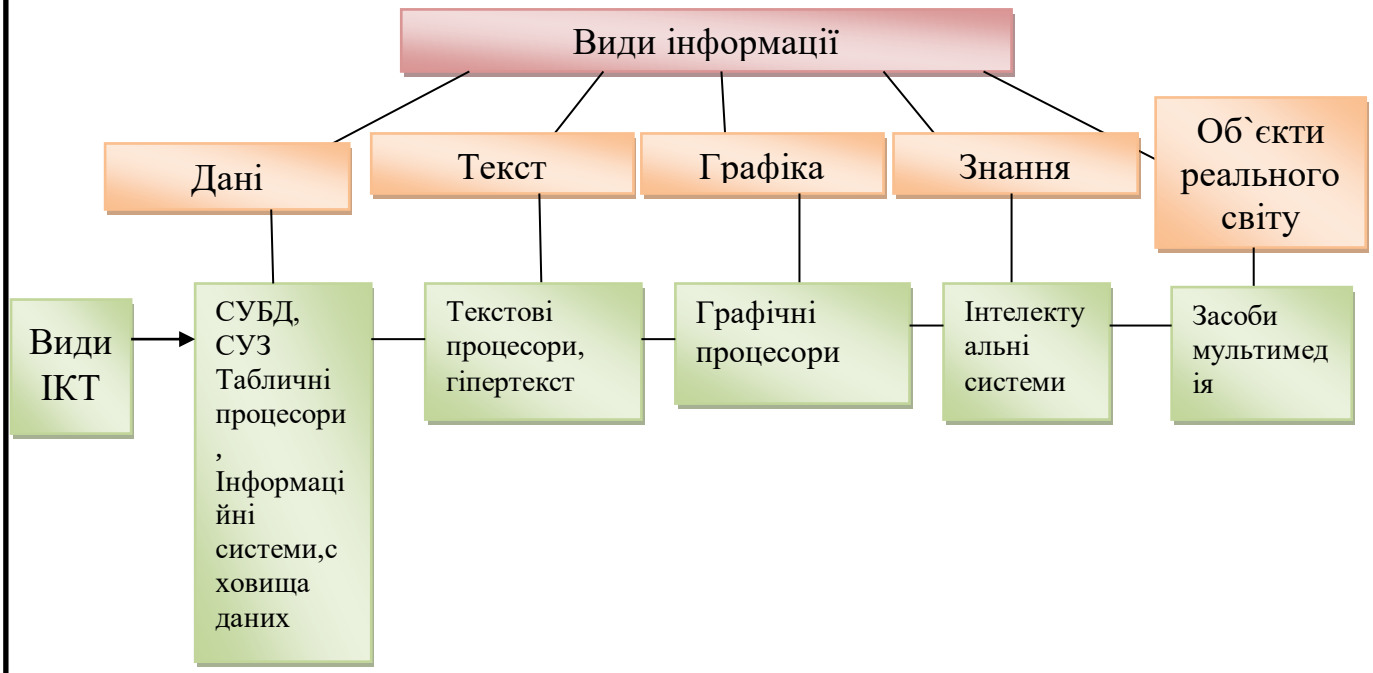

Рис. 1.2 Використання технологій відповідно до подання інформації

1.1 Апаратні засоби інформаційної системи студії Web-дизайну.

Інформаційні системи, побудовані на базі комп'ютерних мереж, забезпечують хропіння даних; обробку даних; організацію доступу користувачів до даних; передачу результатів обробки даних користувачеві; використання додаткових додатків і ресурсів мережі.Використання можливостей комп'ютерних мереж, зокрема локальної мережі, викликано практичною потребою швидкого обміну різнорідною інформацією, одночасного використання прикладних програм, спільного використання ресурсів комп'ютерів і периферійного обладнання, підключеного до мережі, і т.д. Локальна комп'ютерна мережа створюється для об'єднання в робочі групи до декількох десятків, сотень комп'ютерів в рамках однієї, двох або кількох організацій. Зокрема, у всіх освітніх установах використовуються переваги локальних комп'ютерних мереж, що об'єднують комп'ютери різних навчальних аудиторій, які в свою чергу теж знаходяться в локальній мережі в рамках тієї чи іншої аудиторії.

Для організації локальної мережі кожен комп'ютер повинен володіти мережевим адаптером або мережевою картою, які встановлюються в слот розширення материнської плати (або використовуються материнські плати з вбудованими мережевими адаптерами). Фізичне з'єднання комп'ютерів здійснюється за допомогою різних типів кабелів (коаксіальний кабель, вита пара, оптоволоконний кабель і ін.). Швидкість передачі даних в сучасних локальних мережах коливається в діапазоні від 10 Мбіт / с до 1 Гбіт / с. Локальна комп'ютерна мережа являє собою сукупність серверів і робочих станцій. Обробка даних в комп'ютерних мережах розподілена зазвичай між двома об'єктами: клієнтом і сервером. **Клієнт** - задача, робоча станція або користувач комп'ютерної мережі. У процесі обробки даних клієнт може сформувати запит на сервер для виконання складних процедур, читання з файлу, пошуку інформації в базі даних і т.д. Архітектура клієнт-сервер може використовуватися як в однорангових локальних мережах, так і в мережах з ієрархічною структурою

(виділений сервер). Технології взаємодії комп'ютерів, об'єднаних в локальну мережу, можуть відрізнятися в залежності від принципу організації структури мережі, а саме розрізняють однорангові і ієрархічні мережі.

Пристрої з’єднуються в мережу за допомогою спеціального мережевого обладнання. З’єднання може бути **бездротовим** або **кабельним**

Бездротове з'єднання забезпечує передачу даних без допомоги дротів.

Найбільш поширені:

- Wi-Fi
- Bluetooth
- Стільникові мережі.

Bluetooth —

технологія бездротового зв’язку, що забезпечує безкоштовний і надійний о бмін даними між персональними комп’ютерами, мобільними телефонами, принтерами, цифровими фотоапаратами, мишами, клавіатурами, навушниками тощо в радіусі до 10 м.

Зв'язок **Wi-Fi** діє на відстані кількох десятків метрів і використовується для організації бездротових локальних мереж вдома, у класі, в офісі.

Щоб комп’ютер міг передавати або отримувати дані з локальної мережі, він має бути оснащений **мережевою картою.**

Рис. 1.3 Мережева карта

У кабельних мережах комп’ютери з’єднуються один з одним за допомогою **мережевих кабелів.**

Рис 1.4 Мережеві кабеля

Пристрій, що призначений для з’єднання всіх комп’ютерів у локальній мережі, називається мережевим **комутатором** або **роутером.**

Рис 1.5 Мережний роутер

Комп’ютер у мережі виконує одну з функцій: або надає мережеві ресурси, або використовує їх.

Комп’ютер, який надає ресурси, називають сервером. Комп’ютер, який використовує ресурси, називають клієнтом, або робочою станцією.

Інтернет — глобальна комп’ютерна мережа, що складається з мільйонів комп’ютерів у всьому світі.

Провайдер (від англ. provider — постачальник) — це організація, що надає послуги, пов’язані з доступом до глобальної мережі.

Разом із IP-адресою комп’ютерів для адресації ресурсів в Інтернеті використовують доменні імена.

Доменне ім’я — текстова адреса комп’ютера або іншого ресурсу в Інтернеті.

Доменне ім’я складається з назв кількох доменів, відокремлених крапками.

Останнім у доменному імені є домен першого (верхнього) рівня, який зазвичай вказує тип організації чи державу; назва домену другого рівня найчастіше є ім’ям сервера даних; найпершим зліва є власне ім’я ресурсу.

school.regionserv.ua

ua — домен 1 рівня

regionserv — домен 2 рівня

school — домен 3 рівня

Глобальні мережі (ГВП) (Wide Area Network - WAN) складаються з великої кількості комп'ютерів-вузлів, що знаходяться в різних містах, регіонах, країнах. Для створення глобальних мереж зазвичай використовуються вже існуючі лінії зв'язку. Це дозволяє значно знизити вартість, тому що не потрібно прокладати спеціальних ліній зв'язку на великі відстані. Крім того, такий підхід дозволяє зробити глобальні мережі доступними для величезного числа користувачів. Для створення подібних мереж використовуються різні технології передачі інформації. Найбільш часто використовують оптичні, радіорелейні та супутникові лінії зв'язку. ГВП будують в інтересах організацій для внутрішньокорпоративного обміну інформацією, а також для операторів зв'язку, що надають послуги доступу до глобальних мереж або забезпечують взаємодію підрозділів компанії за допомогою зовнішніх мереж.

Основними використовуваними протоколами є TCP / IP, SONET / SDH, MPLS, ATM і Frame relay. Однак принцип використання систем зв'язку загального користування має й істотні недоліки. Низькі швидкості

використовуваних каналів значно звужують спектр пропонованих послуг. Для стійкої передачі даних по лініях зв'язку невисокої якості використовуються спеціальні методи і засоби (зокрема, складні процедури контролю цілісності і відновлення даних). Подібні методи є відмінними ознаками глобальних мереж. Основу глобальної мережі складають обчислювальні системи великої потужності, призначені для одночасної роботи багатьох користувачів, - так звані host-вузли. Спеціальні комп'ютери - комунікаційні вузли - також є необхідною складовою глобальних мереж. Передавальне обладнання глобальних мереж призначене для роботи у звичайних телефонних мережах, а також виділених лініях, таких як Т-лінії та ISDN-лінії. Вони можуть мати аналогові компоненти (наприклад модеми) або повністю цифрові (як для ISDN-комунікацій). Найчастіше це устаткування або перетворює сигнал передачі великі відстані, або створює безліч каналів всередині однієї комунікаційної середовища, забезпечуючи цим вищу пропускну спроможність. Основні види передавального обладнання глобальних мереж:

- мультиплексори;
- групи каналів;
- приватні телефонні мережі;
- телефонні модеми;
- адаптери ISDN;
- кабельні модеми;
- модеми та маршрутизатори DSL;
- сервери доступу;
- маршрутизатори.

Мультиплексори

Мультиплексори (multiplexer, MUX) – це мережні пристрої, які можуть приймати сигнал від безлічі входів та передавати їх у загальне мережеве середовище.

Рис 1.6 Мультиплексор

Мультиплексори по суті є комутаторами і використовуються в старих і нових технологіях, у тому числі:

- у телефонії для комутації фізичних ліній;
- при комутації телекомунікаційних віртуальних ланцюгів для створення безлічі каналів в одній лінії (наприклад, Т-лініях);
- у послідовних каналах для підключення кількох терміналів до однієї лінії (у локальних чи глобальних мережах), навіщо ця лінія ділиться на кілька каналів;
- в технологіях Fast Ethernet, X.25, ISDN, ретрансляції кадрів, ATM других (для створення безлічі комунікаційних каналів в одному кабельному середовищі).

Мультиплексори працюють на Фізичному рівні OSI, перемикаючись між каналами. При цьому використовується один із трьох методів електричної комутації або єдиний метод при передачі оптичного середовища.

Групи каналів

При появі групи каналів (channel bank) або канальні групи являли собою пристрої, що дозволяють пропускати кілька вхідних речових сигналів по одній лінії, а мультиплексори перетворювали кілька сигналів даних для передачі по одній лінії.

Рис 1.7 Групи каналів

Необхідність передачі голосу, даних та відео призвела до швидкого розвитку телекомунікаційних груп каналів, і в даний час за їх допомогою можна як передавати речові сигнали, так і виконувати мультиплексування даних, мовлення та відео. Таким чином, група каналів – це великий мультиплексор, що поєднує телекомунікаційні канали в одному місці, яке називається точкою присутності (point of presence, POP). Ці канали можуть бути приватні лінії T-1, повні лінії T-1 і T-3, ISDN канали або канали з ретрансляцією кадрів. Перші групи каналів типу D-1 складалися з мультиплексорів T-1.

Приватні телефонні мережі

Деякі організації, щоб зменшити кількість ліній, підключених до регіональної телефонної компанії, розгортають свої телефонні служби. Наприклад, компанія може мати 100 офісів, які мають власні телефони, але при цьому не більше 50 співробітників можуть одночасно дзвонити за межі цих офісів. Ця компанія може заощадити кошти, встановивши свою телефонну систему, що має 100 ліній зв'язку з офісами, що підключаються до центральної АТС (автоматичної телефонної станції) або комутаційного вузла, який 50 лініями з'єднаний з регіональною телефонною компанією.

Первоначально наиболее распространенными частными системами были офисные станции с исходящей и входящей связью (private branch exchange, PBX). Они представляли собой коммутаторы с ручным управлением, для которых требовался оператор, выполняющий соединения внутри организации или при выходе во внешнюю телефонную сеть. В результате усовершенствований появились автоматические учрежденческие телефонные системы, называемые частными АТС без выхода в общую сеть (private automatic exchange, PAX) и частными АТС с исходящей и входящей связью (private automatic branch exchange, PABX).

Рис. 1.8 Private automatic branch exchange, PABX

У PABX-станціях, як і раніше, використовується комутатор, і перемикання виконуються як вручну, так і автоматично. У PAX-станціях комутатор відсутня. До складу станцій обох типів входять телефонні магістральні лінії (подібні магістралі мережі), звичайні телефонні лінії, лінії зв'язку з регіональною телефонною компанією, телефони та система комутування на базі процесора або комп'ютер, що має пам'ять, жорсткий диск і програмне забезпечення. Ці станції можуть окрім мови передавати відеосигнали та дані.

Телефонні модеми

Модеми довго грали значної ролі у становленні глобальних мереж. Термін модем є скорочення терміну “модулятор/демодулятор”.

Модем перетворює вихідний комп'ютерний (цифровий) сигнал аналоговий, який може бути переданий по телефонній лінії. Крім того, модем перетворює вхідний аналоговий сигнал на цифровий, зрозумілий комп'ютеру.

Рис. 1.9 Телефонний модем

Модеми для комп'ютерів бувають внутрішні та зовнішні. Внутрішній модем вставляється у комп'ютерний слот розширення материнської платі.

Зовнішній модем – це автономний пристрій, який підключається до послідовного порту комп'ютера за допомогою спеціального модемного кабелю, що збігається з гніздом послідовного порту.

Швидкість передачі даних через модем вимірюється двома схожими, але не ідентичними одиницями: швидкістю в бодах (baud rate) та кількістю бітів, що передаються в секунду (біт/с). Швидкість у бодах є кількістю змін за секунду для хвильового сигналу, що передає дані. Ця швидкість достовірно визначала швидкодію модемів за її появі (коли вони могли за кожної зміни сигналу передавати лише одне біт даних).

Модеми працюють або в синхронному або в асинхронному режимі. При синхронних комунікаціях пакети даних, що повторюються, керуються синхросигналом, що починає кожен пакет. В асинхронному режимі дані передаються окремими блоками, розділеними стартовими та стоповими бітами.

Адаптер ISDN

Для підключення комп'ютера до лінії ISDN необхідний пристрій, що нагадує цифровий модем і називається термінальним адаптером (terminal adapter, TA).

Рис 1.10 Адаптер ISDN

Існуючі термінальні адаптери мають майже таку ж вартість, як і високоякісні асинхронні або синхронні модеми, проте їхня швидкість вище (наприклад, від 128 до 512 Кбіт/с).

Термінальні адаптери перетворюють цифровий сигнал на деякий протокол, який підходить для передачі цифрової телефонної лінії. Зазвичай вони мають роз'єм аналогового телефону, за допомогою якого можна підключити звичайний телефон або модем і використовувати їх на цифровій лінії.

Найчастіше обладнання ISDN дозволяє підключатися до однієї телефонної лінії або мідної пари (такого ж дроту, за допомогою якого домашній або офісний телефон з'єднується з телефонною станцією), проте воно забезпечує роздільні канали для комп'ютерних даних та звичайного аналогового голосового зв'язку. Одночасно можна використовувати одну аналогову і одну цифрову лінію, або дві цифрові, або дві аналогові лінії.

Однією з базових вимог сучасності є вчасне забезпечення особи, яка приймає рішення, актуальною інформацією. Не в останню чергу це стало можливим завдяки тому, що називають тепер «другою комп’ютерною революцією» — поєднанню обчислювальних і комунікаційних технологій у рамках глобальної мережі з неосяжним обсягом і необмеженим потенціалом. Сьогодні термін телекомунікації (від грец. tele — далеко та communico — спілкуюся) позначає здатність передавати текст, голос, зображення і навіть нематеріальні активи (грошові кошти) через мережі разом із функціональною інформацією, призначеною для управління комп’ютерними системами.

Комп’ютерні мережі є одним з основних видів телекомунікацій. Комп’ютерна мережа — це сукупність каналів передавання даних і/або засобів комунікації, які з’єднують окремі ЕОМ і дають змогу використовувати спільні програмні й технічні засоби для організації зв’язку. Основним призначенням комп’ютерних мереж є обмін даними; розподіл ресурсів - спільне використання обчислювальних потужностей (ресурсів процесора), периферійних пристроїв (принтерів, графопобудовників) та ін.; розподіл даних і програмних засобів. Узагальнено комп’ютерні мережі можна поділити на 2 великих класи:

- Локальні мережі LAN (Local Area Network).
- Глобальні, віддалені мережі WAN (Wide Area Network).

Клієнт – комп’ютер, який використовує ресурси мережі Сервер – комп’ютер, який надає власні ресурси для використання іншими комп’ютерами. Характеризується: високою швидкістю, великим обсягом пам'яті, постійно працює в мережі. Види ліній зв’язку: кабельні, телефонні, радіо-, супутникові.

1.2 Програмніі засоби інформаційної системи студії Web-дизайну.

Розвиток інформаційних технологій і розширення сфери їх застосування призвели до інтенсивного розвитку програмного забезпечення (ПЗ). Тенденції розвитку ПЗ показують, що динаміка витрат має стійку тенденцію до зростання, близько 20% на рік. Під програмним забезпеченням інформаційних систем розуміють сукупність програмних і документальних засобів для створення й експлуатації систем обробки даних засобами обчислювальної техніки. Залежно від функцій, виконуваних програмним забезпеченням, його можна поділити на 2 групи: системне програмне забезпечення (Рис. 1.11) і прикладне програмне забезпечення (Рис 1.12). Системне ПЗ організує процес обробки інформації в комп'ютері і забезпечує нормальне робоче середовище для прикладних програм. Системне ПЗ настільки тісно пов'язане з апаратними засобами, що його іноді вважають частиною обчислювальної машини.

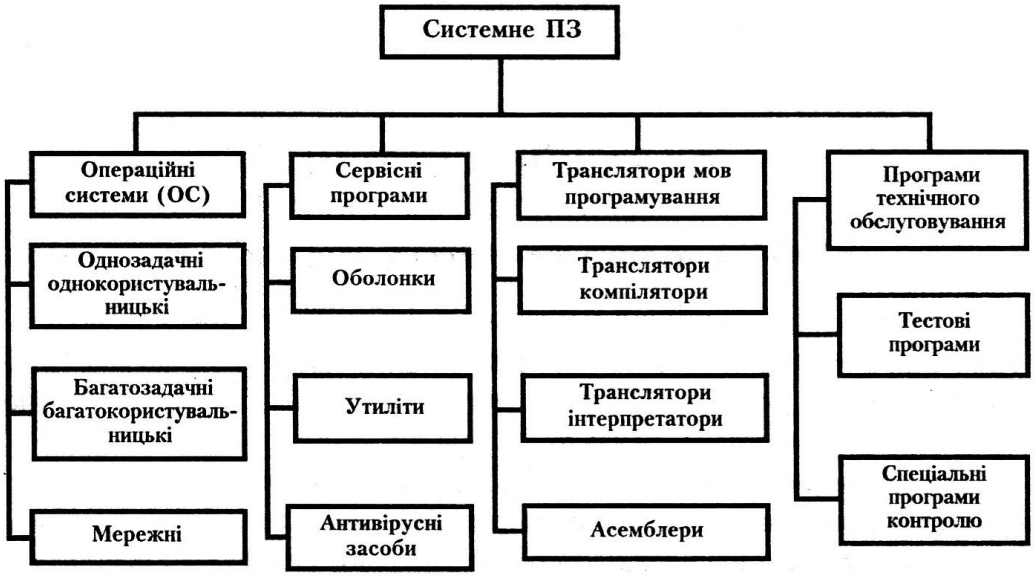

Рис. 1.11 Системне програмне забезпечення

Прикладне ПЗ призначено для вирішення конкретних завдань користувача й організації обчислювального процесу інформаційної системи в цілому.

До складу системного ПЗ входять:

- операційні системи;
- сервісні програми;
- транслятори мов програмування;
- програми технічного обслуговування

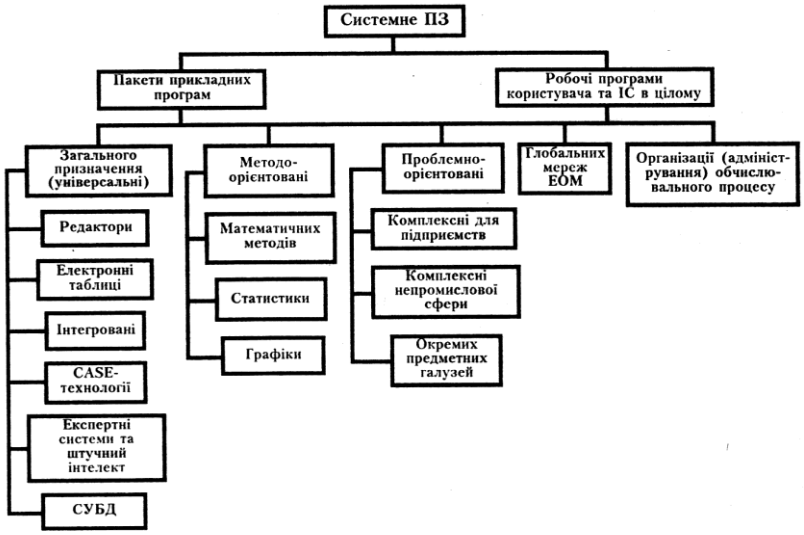

Рис. 1.12 Прикладне програмне забезпечення

Операційні системи (ОС) забезпечують управління процесом обробки інформації і взаємодію між апаратними засобами і користувачем. Однією з найважливіших функцій ОС є автоматизація процесів вводу-виводу інформації, управління виконанням прикладних задач, розв'язуваних користувачем. ОС завантажує потрібну програму в пам'ять ЕОМ і стежить за ходом її виконання; аналізує ситуації, що перешкоджають нормальним обчисленням, і дає вказівки про те, що необхідно зробити, якщо виникли труднощі.

1.2.1 Програмне забезпечення студії Web-дизайна.

Web-сайт є ефективним способом спілкування з клієнтами, і відвідувачі багато разів оцінюють бізнес або послуги на основі Web-сайту. Таким чином веб-сайт відіграє важливу роль у вдосконаленні бізнесу. Щоб мати хороший Web-сайт, слід мати хороше програмне забезпечення для Web-дизайну. Багатофункціональне програмне забезпечення допоможе нам створити багатофункціональний WEb-сайт. Нам потрібні мінімальні навички для створення красивих дизайнів за допомогою відповідного програмного забезпечення для Web-дизайну.

Кілька інструментів Web-дизайну мають можливість автоматизувати весь процес. Web-дизайнери створюють власний набір інструментів, поєднуючи різне програмне забезпечення. Це корисно для створення веб-сайтів для електронної комерції, графічних дизайнерів, маркетологів та HTML-сайтів.

Список найкращих програм для Web-дизайну:

- ADOBE PHOTOSHOP
- ADOBE ILLUSTRATOR
- ADOBE INDESIGN
- ADOBE AFTER EFFECTS

1. **Adobe Photoshop** можна назвати професійною програмою дизайнера. Тому що кожен, хто відчуває у собі творчий потенціал і хоче його реалізувати, створюючи графічний дизайн, має вміти користуватися на дуже високому рівні.

Ми впевнені, що понад 90% наших користувачів та читачів хоч раз користувалися цією програмою для графічних дизайнерів. Якщо Ви хочете краще освоїти цю програму, стати професіоналом, існує безліч різноманітних відеокурсів.

Кожен виділить собі переваги і недоліки цієї програми. Давайте сформулюємо загальні переваги Adobe Photoshop:

- зрозумілий інтерфейс, багато інструментів для роботи, для малювання різних фігур та контурів;
- можливість роботи з 3D-графікою;
- якщо добре знати всі функції та фішки, то можна створювати нереальні речі;
- багато дизайнерів працюють з Photoshop, тому з ними буде легко співпрацювати та обмінюватися файлами;
- відмінно підійде для ретушування, обробки фотографій не тільки на аматорському рівні, але і для якісних знімків;

Але навіть така чудова програма має свої мінуси. Основні з них: преміум версія досить дорога, ліцензію потрібно час від часу активувати, до того ж потрібний досить потужний комп'ютер.

2**. Adobe Illustrator**

Одна з кращих програм для роботи з векторною графікою. З її допомогою створюють іконки, ілюстрації, банери, рекламні листівки, логотипи і забігаючи трохи вперед, макети веб-сайтів. Має багато фішок, наприклад, Touch Type, Free Transform та Puppet Warp.

Векторне зображення можна сильно збільшувати або зменшувати, і воно залишається чітким. Так що в Adobe Illustrator можна легко створити необхідну піктограму або цілий колаж зображень, а потім використовувати їх будь-де і в будь-якому розмірі. Серед недоліків можна назвати відмінності у командах від Photoshop та InDesign, обмежену в часі ліцензію та невелику складність у засвоєнні.

3. **Adobe Indesing**

Вам потрібно зробити плакат, афішу, брошуру, листівку, газету? Тоді вам слід навчатися, працювати в Adobe InDesign. Якщо ви вже знайомі з іншими продуктами від Adobe Systems, можете створювати хороші макети вже через тиждень для вивчення даної програми.

Не великий недолік – більш вузькоспеціалізоване використання цього продукту. Ним користуються частіше ті, хто працює з поліграфією. Незважаючи на це, Adobe InDesign стане в нагоді не тільки дизайнерам, які працюють у видавництві друкованої преси. Програма буде корисна дизайнерам (а може навіть журналістам та блогерам), які верстають веб-журнали. Саме в InDesign'і можна створити чудову обкладинку та цікаві сторінки журналу.

4. **Adobe After Effects**

Модний напрямок дизайну, хоча він існує вже більше століття, моушн-дизайн. Чули? Це рухається на малюнку: пожвавлення фотографій, літер, окремих елементів. Найчастіше цей вид графіки використовують для створення заставок фільмів, реклами чи документального кіно. Кожному дизайнеру буде цікаво та корисно познайомитись з Adobe After Effects, оскільки зараз анімація дійсно у тренді. Плюси: досвідчений дизайнер, розібравшись в інструментах цієї програми, зможе редагувати відеоряд, додавати спецефекти, анімацію, створювати тривимірні картинки. І він ніколи не залишиться без роботи.Мінуси: ціна та той факт, що часто потрібно встановлювати додаткові плагіни.

1.3 Інформація. Дані.Людина

Людські та організаційні чинники можуть бути пов’язані з інформаційною безпекою. Фактори, що впливають на безпеку комп’ютера діляться на дві категорії, а саме людський фактор і організаційний фактор. Людські чинники є важливими, тому їх розділяють на групи **:**

- фактори, які відносяться до управління, а саме робоче навантаження і неякісна робота персоналу;
- фактори, пов’язані з кінцевим користувачем.

Далі ми зосередимося на чотирьох людських факторах, які мають серйозні наслідки впливу на поведінку користувачів.

- Низька мотивація

Керівництво повинно визначати, що мотивує їх персонал.

- Недолік обізнаності

Недолік обізнаності пов’язаний з відсутністю загальних знань про об’єкт, де працює співробітник. Вони не можуть захистити себе від крадіжки особистих даних, а також як контролювати доступ інших користувачів до їх комп’ютера.

- Переконання

Прикладами ризикованого переконання є наступні: вважається, що установка антивірусного програмного забезпечення вирішує проблеми щодо захисту інформації.

- Безграмотне користування технологіями

Навіть найкраща технологія не може досягти успіху у вирішенні проблем інформаційної безпеки без безперервного людського співробітництва та ефективного використання цієї технології. Ризики в області комп’ютерної безпеки можна класифікувати декількома способами: перевищення привілеїв, помилки та упущення, відмова в обслуговуванні, соціальна інженерія, несанкціонований доступ, розкрадання особистих даних, фішинг, шкідливі програми і несанкціоновані копії.

Будь яка велика інформаційна система не може повністю працювати автоматично. Завжди будуть операції для яких процес автоматизації є досить дорогим для організації. Тому, чим більше таких операцій, особливо в основному технологічному ланцюзі роботи КСЗІ, тим більше вона буде залежати від індивідуальних властивостей людини.Людський фактор впливає також на достовірність, своєчасність та повноту обробки інформації, яку вводять та зберігають у базах даних інформаційної системи. При тривалому вводі даних, в процесі втоми, людина починає робити помилки при вводі, пропускати дані, не вкладається в регламентований час.

Вплив людського фактору на достовірність вводу інформації.

	Години роботи					
	1 –а – 6–а	**-а**	**-а**	**-а**	**0-а**	**1-а**
Продуктивність (% від норми)	100	1 04	8	1	4	7
Відсоток		0,				

безпомилковості	96	,9	,85	,78	,71	,64
Реальний час операції, враховуючи повторні роботи (годин)	6,25	,11	,18	,28	,4	,56
Достовірність результатів вводу (відсоток помилок, враховуючи логічні перевірки і повторного вводу)	0,999	,996	,994	,991	,988	,985
Верхня границя достовірності	0,9995	,998	,997	,995	,993	,991
Нижня границя достовірності	0,997	,993	,991	,987	,983	,979

Отже, в таблиці чітко показано, що продуктивність людини суттєво знижується після шостої години роботи. Відповідно негативно впливає на виробництво та захист інформації. Також, зібрані дані в таблиці підтверджують вище написане. Людський фактор важлива складова у кібербезпеці, ІБ та КСЗІ і її побудові.Також, одним із важливих питань в даній проблемі є питання «кваліфікації» співробітника, який обслуговує інформаційну систему. Працівник з низькою кваліфікацією та новачки повинні обов’язково проходити етапи навчання і тренування роботи із системою, яка в свою чергу повинна бути відмінно документована.Людина, безумовно впливає на показники надійності та ефективності (повноти, достовірності, своєчасності обробки інформації) ІС в цілому та її окремих підсистем і задач. Методологія оцінки впливу людського фактору на роботу ІС враховує впливи помилок людини на надійність КСЗІ, а також психологічні особливості людини, як ланки даної системи. Часом дії персоналу обмежують можливість запобігання початковій несправності, що в подальшому переростає в аварійну ситуацію.

Проте, необхідно ідентифікувати різноманітні типи помилкових дій:

- помилка через неуважність, помилку, що вилився в невиконанні необхідної дії інформаційної системи;
- помилка невідповідності, яка може передбачати: становище, коли необхідні дії не виконується належним чином (наприклад, не виконання регламенту адміністрування бази даних);

- дія, що виконується занадто великим або занадто малим зусиллям, або без необхідної точності (наприклад, неточності при заповненні форм введення, помилки неточного введення даних і т.д.);
- дія, що виконується в невідповідний для нього час (наприклад, несвоєчасне введення інформації, затримка обробки інформації і т.д.);
- дія, що виконується з порушенням черговості виконання (наприклад, підготовка підсумкового аналітичного звіту при незавершеному процесі обробки даних);
- зайва дія, що виконується замість необхідної дії або на додаток до нього (наприклад, повторні введення одних і тих же відомостей, що може привести до розбіжностей у відомостях або появою дублюючих даних).

Наслідком є те, що інформаційна безпека є ключем до зменшення загроз в інформаційній безпеці та кібербезпеці, які виникають в наслідок неправильних дій персоналу. Організації повинні розвивати і підтримувати культуру, в якій цінують позитивну поведінку в області інформаційної безпеки. Підприємствам, необхідно підтримувати вектор спрямований на контроль кожної людини в організації, задля підвищення загальної безпеки та продуктивності.

2. 2. Інформаційна безпека студії Web-дизайну

2.1 Несанкціонований доступ до інформації і його мета

Спосіб несанкціонованого доступу (НСД) - це сукупність прийомів і порядок дій з метою одержання (добування) інформації, що охороняється, незаконним протиправним шляхом і забезпечення можливості впливати на цю інформацію (наприклад: підмінити, знищити і т.п.).

При здійсненні несанкціонованого доступу, зловмисник переслідує три мети:

одержати необхідну інформацію для конкурентної боротьби;

мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;

завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей. Повний обсяг даних про діяльність конкурента не може бути отриманий тільки яким-небудь одним з можливих способів доступу до інформації. Від мети залежить як вибір способів дій, так і кількісний і якісний склад сил і засобів добування інформації.

Порушники безпеки інформації. Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як «комп'ютерне піратство».

Для запобігання можливих загроз, фірми повинні не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але і спробувати виявити категорії порушників і ті методи, які вони використовують. У залежності від мотивів, мети і методів, дії порушників безпеки інформації можна розділити на чотири категорії:

- шукачі пригод;
- ідейні «хакери»;

- «хакери»-професіонали;
- ненадійні (неблагополучні) співробітники.

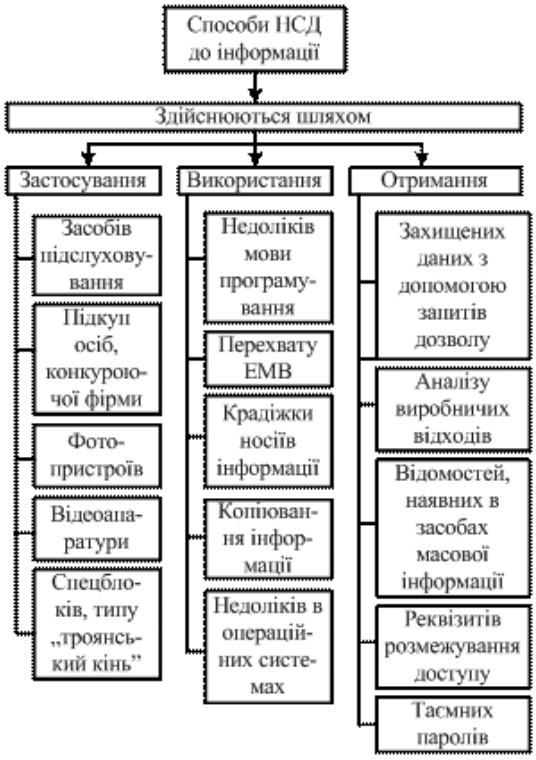

Рис. 2.1 Способи НСД до конфіденційної інформації

Шукач пригод, як правило, студент або старшокласник, і в нього рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись зі складнощами. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами. Ідейний «хакер» - це той же шукач пригод, але більш майстерний. Він уже вибирає собі конкретні цілі (хости і ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Web-сервера або, у більш рідких випадках, блокування роботи ресурсу, що атакується. У порівнянні із шукачем пригод, ідейний «хакер» розповідає про успішні атаки набагато більш широкої аудиторії, звичайно розміщаючи інформацію на хакерському Web-вузлі. «Хакер»-професіонал має чіткий план дій і націлюється на визначені ресурси. Його атаки

добре продумані і звичайно здійснюються в кілька етапів. Спочатку він збирає попередню інформацію (тип ОС, надані сервіси і міри захисту). Потім він складає план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Далі, провівши атаку, він одержує закриту інформацію і, нарешті, знищує всі сліди своїх дій. Такий професіонал звичайно добре фінансується і може працювати один або в складі команди професіоналів. Ненадійний (неблагополучний) співробітник своїми діями може спричинити стільки ж проблем (буває і більше), скільки промисловий шпигун, до того ж, його присутність звичайно складніше знайти. Крім того, йому доводиться переборювати не зовнішній захист мережі, а тільки, як правило, менш жорсткіший внутрішній. Він не такий витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки і тим самим може видати свою присутність.

Однак, у цьому випадку, небезпека його несанкціонованого доступу до корпоративним даних набагато вища, ніж будь-якого іншого зловмисника. Перераховані категорії порушників безпеки інформації можна згрупувати по їхній кваліфікації: початківець (шукач пригод), фахівець (ідейний «хакер», ненадійний співробітник), професіонал («хакер»-професіонал). А якщо з цими групами зіставити мотиви порушення безпеки і технічну оснащеність кожної групи, то можна одержати узагальнену модель порушника безпеки інформації, як це показано на (рис. 2.2)Порушник безпеки інформація, як правило, будучи фахівцем визначеної кваліфікації, намагається довідатися все про комп'ютерні системи і мережі, зокрема, про засоби їх захисту. Тому модель порушника визначає: категорії осіб, у числі яких може виявитися порушник;

· можливі цілі порушника і їх градації по ступені важливості і небезпеки;

· припущення про його кваліфікації;

· оцінка його технічної озброєності;

· обмеження і припущення про характер його дій.

Діапазон спонукальних мотивів одержання доступу до системи досить широкий: від бажання випробувати емоційний підйом під час гри з комп'ютером до відчуття влади над ненависним менеджером. Займаються цим не тільки новачки, що бажають побавитися, але і професійні програмісти. Паролі вони добувають, або в результаті підбору або здогадування, або шляхом обміну з іншими «хакерами». Частина з них, однак, починає не тільки переглядати файли, але і виявляти інтерес саме до їх змісту, а це вже являє серйозну загрозу, оскільки в даному випадку важко відрізнити звичайну цікавість від злочинних дій.

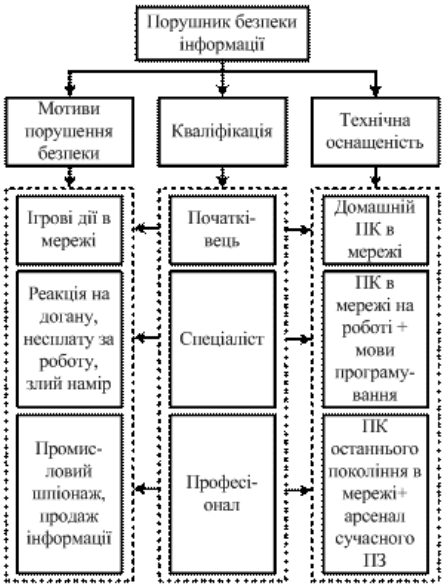

Рис. 2.2 Модель порушника безпеки інформації.

Донедавна викликали занепокоєння випадки, коли незадоволені керівником службовці, зловживаючи своїм положенням, псували системи, допускаючи до них сторонніх або залишаючи системи без догляду в робочому стані. Спонукальними мотивами таких дій є:

· реакція на догану або зауваження з боку керівника;

· невдоволення тим, що фірма не оплатила понаднормові години роботи (хоча найчастіше понаднормова робота виникає через неефективне використання робочого часу);

· злий намір у якості, наприклад, реваншу з метою послабити фірму як конкурента якої-небудь новоствореної фірми.

2.2 Поняття інформаційної безпеки

Під інформаційною безпекою розуміється захищеність інформації та інфраструктури, що її підтримує, від будь-яких випадкових або зловмисних впливів, результатом яких може стати заподіяння шкоди самої інформації, її власникам або підтримуючій інфраструктурі. Завдання інформаційної безпеки зводяться до мінімізації збитків, а також до прогнозування та запобігання таким впливам. Параметри інформаційних систем, що потребують захисту, можна розділити на такі категорії: забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів.

доступність - це можливість отримання за короткий проміжок часу необхідної інформаційної послуги;

цілісність - це актуальність та несуперечність інформації, її захищеність від руйнування та несанкціонованої зміни;

конфіденційність - захист від несанкціонованого доступу до інформації.

Інформаційні системи, перш за все, створюються для отримання певних інформаційних послуг. Якщо отримання інформації з будь-яких причин стає неможливим, це завдає шкоди всім суб'єктам інформаційних відносин. З цього можна визначити, що доступність інформації стоїть першому місці. Цілісність є основним аспектом інформаційної безпеки тоді, коли точність та правдивість будуть головними параметрами інформації. Наприклад, рецепти медичних ліків або набір та характеристики комплектуючих виробів. Події, які можуть завдати шкоди інформаційній системі, можна поділити на кілька

категорій: цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачем внаслідок необережних дій."Електронні" методи впливу, що здійснюються хакерами. Під хакерами розуміються люди, котрі займаються комп'ютерними злочинами як професійно (зокрема у межах конкурентної боротьби), і просто з цікавості. До таких методів належать:

несанкціоноване проникнення у комп'ютерні мережі; Метою несанкціонованого проникнення ззовні в мережу підприємства може бути завдання шкоди (знищення даних), крадіжка конфіденційної інформації та використання її в незаконних цілях, використання мережевої інфраструктури для організації атак на вузли третіх фірм, крадіжка коштів з рахунків тощо. Система управління інформаційною безпекою (ISMS або Information Security Management System) дозволяє керувати комплексом заходів, що реалізують якусь задуману стратегію, в даному випадку щодо інформаційної безпеки. Зазначимо, що йдеться не лише про управління вже існуючою системою, а й про побудову нового/перепроектування старої. Комплекс заходів включає у собі організаційні, технічні, фізичні та інші. Управління інформаційною безпекою (ІБ) - процес саме комплексний, що дозволяє реалізовувати якомога ефективніше і всебічне управління ІБ у компанії.

Мета управління ІБ полягає у збереженні конфіденційності, цілісності та доступності інформації. Питання тільки в тому, яку саме інформацію необхідно охороняти та які зусилля докладати для забезпечення її безпеки. Будь-яке управління ґрунтується на усвідомленні ситуації, в якій воно відбувається. У термінах аналізу ризиків усвідомлення ситуації виявляється у інвентаризації та оцінці активів організації та його оточення, т. е. всього, що забезпечує ведення бізнес-діяльності. З погляду аналізу ризиків ІБ до основних активів відносяться безпосередньо інформація, інфраструктура, персонал, імідж та репутація компанії. Без інвентаризації активів лише на рівні бізнес-діяльності неможливо відповісти питанням, що саме потрібно захищати. Дуже важливо

зрозуміти, яка інформація обробляється в організації та де виконується її обробка. У разі великої сучасної організації кількість інформаційних активів може бути дуже велика. Тому першочерговим завданням управління ризиками стає визначення найзначніших активів. Вирішити це завдання неможливо без залучення менеджерів основного напряму діяльності організації як середньої, і вищої ланки. Оптимальна ситуація, коли вищий менеджмент організації особисто ставить найбільш критичні напрямки діяльності, для яких дуже важливо забезпечити інформаційну безпеку. Думка вищого керівництва з приводу пріоритетів у забезпеченні ІБ дуже важлива і цінна в процесі аналізу ризиків, але у будь-якому разі вона має уточнюватися шляхом збору відомостей про критичність активів на середньому рівні управління компанією. При цьому подальший аналіз доцільно проводити саме за позначеними вищим менеджментом напрямками бізнес-діяльності. Отримана інформація обробляється, агрегується та передається вищому менеджменту для комплексної оцінки ситуації. Робота з визначення цінності інформаційних активів у межах всієї організації одночасно найбільш значуща і складна. Саме оцінка інформаційних активів дозволить начальнику відділу ІБ обрати основні напрямки діяльності із забезпечення інформаційної безпеки. Але економічна ефективність процесу управління ІБ багато в чому залежить саме від усвідомлення того, що потрібно захищати і які зусилля для цього знадобляться, так як у більшості випадків обсяг зусиль, що докладаються, прямо пропорційний обсягу витрачених грошей і операційних витрат. Управління ризиками дозволяє відповісти на питання, де можна ризикувати, а де не можна. У випадку ІБ термін «ризикувати» означає, що у певній галузі можна не докладати значних зусиль для захисту інформаційних активів і при цьому у разі порушення безпеки організація не зазнає значних втрат. Тут можна провести аналогію з класами захисту автоматизованих систем: що значніші ризики, то жорсткішими мають бути вимоги до захисту. Щоб визначити наслідки порушення безпеки, потрібно мати відомості про зафіксовані інциденти аналогічного характеру, або провести сценарний аналіз. У рамках сценарного аналізу вивчаються причинно-наслідкові

зв'язки між подіями порушення безпеки активів та наслідками цих подій для бізнес-діяльності організації. Наслідки сценаріїв мають оцінюватися кількома людьми, ітераційним чи дорадчим методом. Слід зазначити, що розробка та оцінка таких сценаріїв може бути повністю відірвана від реальності. Завжди слід пам'ятати, що сценарій має бути ймовірним. Критерії та шкали визначення цінності індивідуальні для кожної організації. За результатами сценарного аналізу можна отримати інформацію про цінність активів. Якщо активи ідентифіковані та визначена їхня цінність, можна говорити про те, що мети забезпечення ІБ частково встановлені: визначено об'єкти захисту та значущість підтримки їх у стані інформаційної безпеки для організації.

2.3 Кіберзлочинність: феномен і його прояви.

Терміни «кібербезпека» та «інформаційна безпека» зазвичай використовуються як синоніми в термінології безпеки і створюють плутанину серед фахівців в сфері безпеки.

Сьогодні ми живемо і працюємо у світі глобальних можливостей взаємодії. Стрімке збільшення кількості персональних комп'ютерів, вільний доступ до Інтернету і швидкий розвиток ринку нових комунікаційних пристроїв змінили і способи проведення дозвілля, і методи ведення бізнесу. Змінюються і способи скоєння злочинів. Злочинність глобальних цифрових технологій відкриває нові можливості для діяльності злочинців. І бізнесмени, і споживачі позбавилися мільйонів доларів «за допомогою» злочинців, що володіють комп'ютерними знаннями. Більш того, комп'ютери і мережі можуть використовуватися для того, щоб викликати тривогу, посіяти паніку, очікувати насильницьких нападів – і навіть для координації і здійснення терористичних дій. На жаль, у багатьох випадках правоохоронні органи відстають від злочинців, не маючи необхідних технологій і кваліфікованого персоналу для створення перешкод нової і швидко зростаючої загрози, названої кіберзлочинністю

Термін «кіберзлочинність» у правових актах офіційно не вказується. Разом з тим, саме поняття закріпилося в лексиконі правоохоронних

органів розвинених держав Європи і Світу і має на увазі злочинність у сфері комп'ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

Донедавна багато техніків-професіоналів не розуміли феномена кіберзлочинності й не виявляли інтересу до нього. У багатьох випадках працівники правоохоронних органів відчували недолік інструментарію, необхідного для того, щоб зайнятися цією проблемою

2.4 Загрози інформаційної безпеки

Загроза інформаційної безпеки — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам. Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або опосередковано призвести до заподіяння шкоди даним того чи іншого суб'єкта. Під системою безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз (Рис. 2.3)

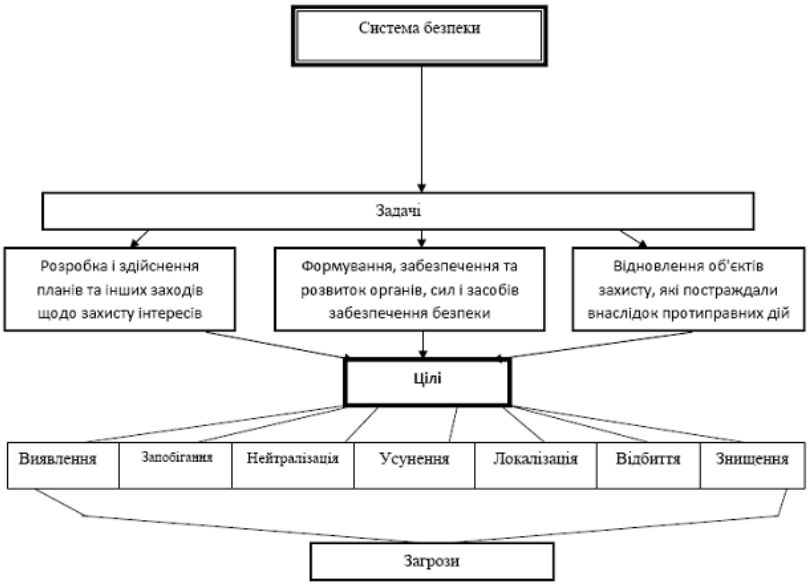

Рис. 2.3 Функціональна система інформаційної безпеки

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мети, а також інші умови і дії, що порушують безпеку .

При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку

Загроза - сукупність факторів та умов, що виникають в процесі взаємодії об'єкта безпеки з іншими об'єктами, а також складових його компонентів між собою і здатних чинити на нього негативний вплив. Вона виступає в якості можливості вирішення протиріччя у взаємодії об'єкта безпеки з іншими об'єктами, компонентів об'єкта безпеки, що у стадії дисгармонії чи конфлікту, шляхом насильницької зміни в бік погіршення властивостей об'єкта безпеки, або його компонентів, тобто шляхом нанесення шкоди. Між загрозою і небезпекою нанесення шкоди завжди існують відносини заподіяння, які визначаються як обумовлена сутністю взаємодіючих об'єктів, елементів системи, зв'язок між явищами, при якій одне явище, зване причиною, за наявності певних умов неминуче породжує, викликає до життя інше явище, зване слідством. Загроза

завжди породжує небезпеку. Небезпека може бути визначена як стан, в якому знаходиться об'єкт безпеки внаслідок появи загрози.

Відмінність між ними полягає в тому, що небезпека є властивістю об'єкта безпеки, а загроза - властивістю об'єкта взаємодії або знаходяться у взаємодії елементів об'єкта безпеки, виступаючих як джерело загроз. Загроза знаходиться у відношенні заподіяння не тільки з небезпекою, але і з очікуваним шкодою - наслідками негативної зміни умов існування, які необхідно подолати для відновлення необхідних умов - в тому сенсі, що очікуваний шкоду визначає величину небезпеки. Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій (наведених в рис. 2.4):

Рис. 2.4 Види загроз інформаційної безпеки

Відповідно до наведеної вище класифікації загроз за видом об'єкта впливу вони поділяються на загрози власне інформації, загрози персоналу

об'єкта та загрози діяльності щодо забезпечення інформаційної безпеки об'єкта. При більш детальному розгляді загроз інформації, їх можна поділити на загрози носіям конфіденційної інформації, місцям їх розміщення (розташування), каналам передачі (системам інформаційного обміну), а також інформації, що зберігається в документованому (електронному) вигляді на різних носіях. За характером порушення, як один із варіантів класифікації, зображено на (рис 2.5)

Таким чином, можна зробити висновок про те, що дія загроз інформаційній безпеці об'єкта направлено на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації.

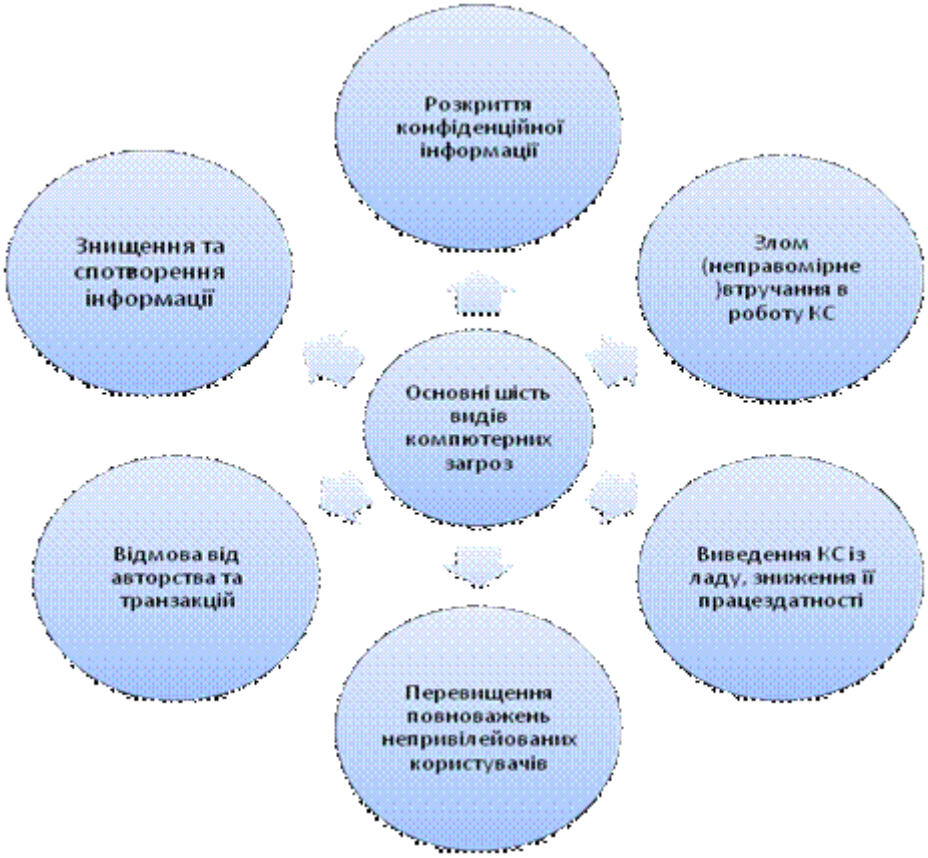

Рис. 2.5 Шість основних загроз інформаційній безпеці (класифікація за характером порушення)

Одне з ключових понять в оцінці ефективності прояви загроз об'єкту інформаційної безпеки - збиток, що наноситься цьому об'єкту (підприємству) в результаті впливу загроз. За своєю суттю будь-який збиток, його визначення та оцінка мають яскраво виражену економічну основу. Не є

винятком і збиток, що наноситься інформаційній безпеці об'єкта студії веб-дизайну.

З позиції економічного підходу, загальний збиток інформаційної безпеки підприємства складається з двох складових частин: прямого і непрямого збитку. Прямий збиток інформаційної безпеки підприємства виникає внаслідок витоку конфіденційної інформації. Непрямий збиток - втрати, які несе підприємство у зв'язку з обмеженнями на поширення інформації, в установленому порядку віднесеної до категорії конфіденційної.

Опис збитку, що наноситься підприємству в результаті витоку конфіденційної інформації, грунтується на його кількісних і якісних показниках, які базуються на одному з принципів засекречування інформації (віднесення її до категорії конфіденційної) - принципі обгрунтованості. Він полягає у встановленні (шляхом експертних оцінок) доцільності засекречування конкретних відомостей, а також ймовірних наслідків цих дій, з урахуванням розв'язуваних підприємством задач і поставлених цілей. Введення обмежень на поширення інформації (у зв'язку з її засекречуванням або віднесенням до категорії конфіденційної) призводить і до позитивних, і до негативних наслідків. До основних позитивних наслідків слід віднести запобігання можливого прямого збитку інформаційної безпеки підприємства через витік інформації, що захищається. Негативні наслідки пов'язані з наявністю (ймовірним зростанням) непрямого збитку або витрат у вигляді витрат на захист інформації та величини упущеної вигоди, яка може бути отримана при її відкритому розповсюдженні. Загальний збиток безпеки підприємства від витоку конфіденційної інформації визначають наступним чином. Проводять класифікацію всіх наявних на підприємстві відомостей за ступенем їх важливості.

З цією метою методом експертної оцінки з залученням фахівців структурних підрозділів підприємства, що беруть участь у виконанні робіт з різних напрямків його діяльності, розробляють єдину шкалу відомостей, що містять конфіденційну інформацію - так званий рейтинг важливості інформації.

У рейтингу відбиваються всі відомості, включені до переліків інформації, що підлягає захисту. Методичною основою для розробки такого рейтингу служить метод експертного аналізу в сукупності з методом об'єктивного кількісного оцінювання. На основі рейтингу важливості інформації зіставляють (співвідносять) включені до нього відомості з кількісними показниками можливого збитку, що визначається розрахунковим або експертним шляхом.

При розробці необхідних, засобів, методів і заходів, що забезпечують захист інформації, необхідно враховувати велику кількість різних факторів. Інформація, будучи предметом захисту, може бути представлена на різних технічних носіях. Її носіями можуть бути люди з числа користувачів і обслуговуючого персоналу. Інформація може піддаватися обробці в комп'ютерних системах, передаватися по каналах зв'язку і відображатися різними пристроями. Вона може розрізнятися за своєю цінністю. Об'єктами, що підлягають захисту, де може перебувати інформація, є не тільки комп'ютери і канали зв'язку, але й приміщення, будівлі та прилегла територія. Істотно різнитися може кваліфікація порушників, а також використовувані способи і канали несанкціонованого доступу до інформації. Таким чином, основними принципами забезпечення інформаційної безпеки є наступні:

Системності.

Комплексності.

Безперервності захисту.

Розумної достатності.

Гнучкості управління і застосування.

Відкритості алгоритмів і механізмів захисту.

Простоти застосування захисних заходів і засобів.

2.5 Безпека інформаційних систем

Під безпекою ІС розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або

фізичного руйнування її' компонентів, тобто здатність протидіяти різним підбурює впливів на ІС. Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Серед загроз безпеки інформації слід виділяти загрози випадкові або ненавмисні, і навмисні. Джерелом випадкових загроз може бути вихід з ладу апаратних засобів, неправильні дії працівників ІС або її користувачів, ненавмисні помилки в програмному забезпеченні і т.д. Такі погрози теж беруть до уваги, тому що збиток від них може бути значним. Загрози умисні на відміну від випадкових переслідують мету нанесення шкоди керованій системі або користувачам. Це робиться нерідко заради отримання особистої вигоди. В даний час для забезпечення захисту інформації потрібна реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно – правових актів, морально – етичних заходів протидії і т.д.). Комплексний характер захисту виникає з комплексних дій зловмисників, що прагнуть будь-якими засобами добути важливу для них інформацію. Реалізація технології захисту інформації в комп'ютерних інформаційних системах і в мережах передачі даних вимагає зростаючих витрат і зусиль. Однак, все це дозволяє уникнути значно переважаючих втрат і збитків, які можуть виникнути при реальному здійсненні погроз ІС та ІТ. Види умисних загроз безпеки інформації:

- 1) Пасивні загрози – спрямовані в основному на несанкціоноване використання інформаційних ресурсів ІС, не надаючи при цьому впливу на її функціонування (наприклад, несанкціонований доступ до баз даних, прослуховування каналів зв'язку і т.д.);
- 2) Активні загрози – мають на меті порушити нормальне функціонування ІС шляхом цілеспрямованого впливу на її компоненти. До активних загроз відносяться, наприклад, виведення з ладу комп'ютера або

його операційної системи, спотворення відомостей в банках даних, руйнування програмного забезпечення комп'ютерів, порушення роботи ліній зв'язку і т.д. Джерелом активних загроз можуть бути дії зломщиків, шкідливі програми і т.п.

Крім того, умисні загрози поділяються на внутрішні (що виникають всередині керованої організації) і зовнішні.

Внутрішні загрози найчастіше визначаються соціальною напруженістю і важким моральним кліматом. Зовнішні загрози можуть визначатися зловмисними діями конкурентів, економічними умовами та іншими причинами (наприклад стихійними лихами). За даними зарубіжних джерел, широке розповсюдження сьогодні отримало промислове шпигунство – це нанесення збитку власникові комерційної таємниці особою, що не уповноважена на це її власником. Це здійснюється за допомогою незаконного збору, привласнення і передачі відомостей, що становлять комерційну таємницю. До основних загроз безпеки інформації і нормального функціонування ІС відносяться:

- – витік конфіденційної інформації;
- – компрометація інформації;
- – несанкціоноване використання інформаційних ресурсів;
- – помилкове використання інформаційних ресурсів;
- – несанкціонований обмін інформацією між абонентами;
- – відмова від інформації;
- – порушення інформаційного обслуговування;
- – незаконне використання привілеїв.

Витік конфіденційної інформації – це безконтрольний вихід конфіденційної інформації за межі ІС або кола осіб, яким вона була довірена по службі або стала відома в процесі роботи. Цей витік може бути наслідком:

- – розголошення конфіденційної інформації;

- – виходу інформації з різних, головним чином, технічних каналів;
- – несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошення інформації її власником або володарем – це умисні або необережні дії посадових осіб або користувачів (яким відповідні відомості в установленому порядку були довірені по службі чи по роботі), внаслідок яких особи, не допущені до інформації, все ж з нею ознайомилися.

Можливий безконтрольний витік конфіденційної інформації з візуально – оптичних, акустичних, електромагнітних й інших каналів. Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, не має права доступу до охоронюваним відомостями. Методи забезпечення безпеки інформації в ІС:

- – перешкода;
- – управління доступом;
- – механізми шифрування;
- – протидія атакам шкідливих програм;
- – регламентація;
- – примус;
- – спонукання.

Перешкода – метод фізичних перешкод шляху зловмиснику до інформації, що захищається (до апаратури, носіям інформації і т.д.). Управління доступом – методи захисту інформації регулюванням використання всіх ресурсів ІС та ІТ. Ці методи повинні протистояти всім можливим шляхам несанкціонованого доступу до інформації. Управління доступом включає наступні функції захисту:

- – ідентифікацію користувачів, персоналу і ресурсів системи (привласнення кожному об'єкту персонального ідентифікатора);
- – впізнання (встановлення автентичності) об'єкту або суб'єкта по пред'явленому їм ідентифікатору;
- – перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);
- – дозвіл і створення умов роботи в межах встановленого регламенту;
- – реєстрацію (протоколювання) звернень до ресурсів, що захищаються

реагування (сигналізація, відключення, затримка робіт, відмова в запиті тощо) при спробах несанкціонованих дій.

Механізми шифрування – криптографічне закриття інформації. Ці методи захисту все ширше застосовуються як при обробці, так і при зберіганні інформації на магнітних носіях. При передачі інформації по каналах зв'язку великої протяжності цей метод є єдино надійним. Протидія атакам шкідливих програм передбачає комплекс різноманітних заходів організаційного характеру і використання антивірусних програм. Цілі прийнятих заходів – це зменшення ймовірності інфікування АІС, виявлення фактів зараження системи; зменшення наслідків інформаційних інфекцій, локалізація або знищення вірусів; відновлення інформації в ІС. Оволодіння цим комплексом заходів і засобів вимагає знайомства зі спеціальною літературою. Регламентація – створення таких умов автоматизованої обробки, зберігання та передачі інформації, яка захищається, при яких норми і стандарти цього захисту виконуються в найбільшою мірою.

Примус – метод захисту, при якому користувачі та персонал ІС змушені дотримуватися правил обробки, передачі і використання інформації, що захищається під загрозою матеріальної, адміністративної чи кримінальної відповідальності. Спонукання – метод захисту, що спонукає користувачів і

персонал ІС не порушувати встановлені порядки за рахунок дотримання сформованих моральних і етичних норм. Вся сукупність технічних засобів захисту поділяється на апаратні і фізичні. Апаратні засоби – пристрої, що вбудовуються безпосередньо в обчислювальну техніку, або пристрої, які сполучаються з нею по стандартному інтерфейсу. Фізичні засоби включають різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту та здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій. Приклади фізичних коштів: замки на дверях, грати на вікнах, засоби електронного охоронної сигналізації тощо. Програмні засоби – це спеціальні програми і програмні комплекси, призначені для захисту інформації в ІС. Як зазначалося, багато з них злиті з ПЗ самої ІС. Із засобів ПЗ системи захисту виділимо ще програмні засоби, що реалізують механізми шифрування (криптографії). Криптографія – це наука про забезпечення таємності і / або автентичності (справжності) переданих повідомлень. Організаційні засоби здійснюють своїм комплексом регламентацію виробничої діяльності в ІС та взаємовідносини виконавців на нормативно – правовій основі таким чином, що розголошення, витік і несанкціонований доступ до конфіденційної інформації стає неможливим або істотно ускладнюється за рахунок проведення організаційних заходів. Комплекс цих заходів реалізується групою інформаційної безпеки, але повинен перебувати під контролем першого керівника. Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, обробки і передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил.

3. Комплексна система захисту інформації студії Web-дизайну

3.1 Заходи безпеки інформаційних систем

Забезпечення безпеки інформації у інформаційно-телекомунікаційних системах здійснюється шляхом створення та впровадження комплексних систем захисту інформації. Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від несанкціонованого доступу.

Існує думка, що проблеми захисту інформації стосуються виключно інформації, що обробляється комп'ютером. Це, мабуть, пов'язано з тим, що комп'ютер і, зокрема, персональний комп'ютер є «ядром», центром зберігання інформації. Об'єкт інформатизації, стосовно до якого спрямовані дії щодо захисту інформації, видається більш широким поняттям порівняно з персональним комп'ютером. У реальному житті всі ці окремі “об'єкти інформатизації” розташовані в межах одного підприємства і являють собою єдиний комплекс компонентів, пов'язаних спільними цілями, завданнями, структурними відносинами, технологією інформаційного обміну і т. д.

Сучасне підприємство – велика кількість різнорідних компонентів, об'єднаних в складну систему для виконання поставлених цілей, які в процесі функціонування підприємства можуть модифікуватися. Різноманіття та складність впливу внутрішніх та зовнішніх чинників, які часто не піддаються чіткому кількісному оцінюванню, призводять до того, що ця складна система може набувати нові якості, не властиві її складовим компонентів. Характерною особливістю подібних систем є насамперед наявність людини в кожній з складових підсистем і віддаленість людини від об'єкта її діяльності. Це відбувається у зв'язку з тим, що безліч компонентів, які складають об'єкт інформатизації, інтегрально може бути подано сукупністю трьох груп систем: 1) люди (біосоціальні системи); 2) техніка (технічні системи та приміщення, в яких вони розташовані); 3) програмне забезпечення, яке є інтелектуальним

посередником між людиною і технікою (інтелектуальні системи). Сукупність цих трьох груп утворює соціотехнічну систему. Таке уявлення про соціотехнічну систему є досить поширеним і може стосуватися багатьох об'єктів. Коло наших інтересів обмежується дослідженням безпеки систем, призначених для обробки вхідної на їх вхід інформації і видачі результату. Розглянемо основні особливості сучасного підприємства:

– складна організаційна структура;

– багатоаспектність функціонування;

– висока технічна оснащеність;

– широкі зв'язки з кооперації;

– необхідність розширення доступу до інформації;

– зростаюча питома вага цифрової технології обробки інформації;

- зростаюча питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;

- важливість і відповідальність рішень, прийнятих в автоматизованому режимі, на основі автоматизованої обробки інформації;

- висока концентрація в автоматизованих системах інформаційних ресурсів;

- велике територіальне розподілення компонентів автоматизованих систем;

- накопичення на технічних носіях величезних обсягів інформації;

- інтеграція в єдиних базах даних інформації різного призначення і різної належності;

- довгострокове зберігання великих обсягів інформації на машинних носіях;

- безпосередній і одночасний доступ до ресурсів (також і до інформації) автоматизованих систем великого числа користувачів різних категорій і різних установ;

- інтенсивна циркуляція інформації між компонентами автоматизованих систем, також і віддалених один від одного.

Таким чином, створення індустрії переробки інформації, з одного боку, створює об'єктивні передумови для підвищення рівня продуктивності праці та життєдіяльності людини, з іншого боку, породжує цілий ряд складних і великомасштабних проблем. Однією з них є забезпечення збереження і встановленого статусу інформації, що циркулює і оброблюється на підприємстві, в організації. Роботи з захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не вважає, що досить провести на підприємстві ряд організаційних заходів, ввести до складу автоматизованих систем деякі технічні і програмні засоби – і цього буде достатньо для забезпечення безпеки. Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, які використовуються для ЗІ, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру. Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі інформації: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговувального персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи. Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ . На основі теоретичних досліджень і практичних робіт у сфері ЗІ сформульований системно-концептуальний підхід до захисту інформації. Під системністю як основною частиною системно-концептуального походу розуміється:

– системність цільова, захищеність інформації розглядається як основна частина загального поняття якості інформації;

– системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

– системність тимчасова, що означає безперервність робіт із ЗІ, що здійснюються відповідно до планів;

– системність організаційна, що означає єдність організації всіх робіт по ЗІ і управління ними.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт щодо ЗІ. Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Комплексний (системний) підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені такі її компоненти: Вхідні елементи. Це ті елементи, для обробки яких створюється система. Як вхідні елементи виступають види загроз безпеки, можливі на даному об'єкті; Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри і т. д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації; Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі сфер інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій із захисту інформації, переданої сигналами в кабельній лінії, що проходить територіями різних об'єктів. Як би не встановлювались межі системи, не можна ігнорувати її взаємодію з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши,

наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей. Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи; Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декілька варіантів побудови системи, що забезпечують задані цілі функціонування. Для того, щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісне оцінювання на всіх етапах створення системи. Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, цілі захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу. Головна мета створення системи захисту інформації – забезпечення надійності ЗІ. Система ЗІ - це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів. Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого – самі організовують систему, здійснюючи захисні заходи. Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами та пов'язаний з ними логічно і технологічно. Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується. По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як

локальні СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правова, організаційна, інженерно-технічна). По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які забезпечують або можуть впливати на якість захисту. Наприклад, система охоплює якісь об'єктів захисту, а всі вони внесені до неї чи ні – це вже поза межами системи.Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися все, виходячи з цілей і завдань захисту заходу.По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, в всіх місцях її збирання, зберігання, передачі і використання, весь час і при всіх режимах функціонування систем обробки інформації. У той же час комплексність не усуває, а, навпаки, передбачає диференційований підхід до захисту інформації, залежно від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умов прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації полягає у:

– інтеграції локальних систем захисту;

– забезпеченні повноти всіх складових системи захисту;

– забезпеченні всеосяжність захисту інформації.

Виходячи з цього, можна сформулювати таке означення: «Комплексна система захисту інформації – система, що повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї захищуваної інформації». Усвідомлення необхідності розробки стратегічних підходів до захисту формувалося в міру усвідомлення важливості, натхнення і проблеми захисту, а також неможливості ефективного її здійснення простим використанням деякого набору засобів захисту.

Під стратегією взагалі розуміється загальна спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб в даному виді діяльності, потенційно можливих умов її здійснення і можливостей організації. Відомий канадський фахівець у сфері стратегічного управління Г. Мінцберг запропонував визначення стратегії в рамках системи «5-Р». На його думку, вона містить:

1) план (Plan) - заздалегідь намічені в деталях і контрольовані дії на певний термін, що переслідують конкретні цілі;

2) прийом, або тактичний хід (Ploy), що є короткочасною стратегією, яка має обмежені цілі, спроможна змінюватися та маневруввати з метою використати їх проти противника;

3) модель поведінки (Patten of behaviour) – часто спонтанну, неусвідомлену, що не має конкретних цілей;

4) позицію щодо до інших (Position in respect to others);

5) перспективу (Perspective).

Завдання стратегії полягає в створенні конкурентної переваги, усунення негативного ефекту нестабільності навколишнього середовища, забезпеченні прибутковості, врівноваженні зовнішніх вимог і внутрішніх можливостей. Через її призму розглядаються всі ділові ситуації, з якими організація стикається в

повсякденному житті. Здатність компанії, організації проводити самостійну стратегію в усіх сферах робить її більш гнучкою, стійкою, дозволяє адаптуватися до вимог часу і обставин. Стратегія формується під впливом внутрішнього і зовнішнього середовищ, постійно розвивається, бо завжди виникає щось нове, на що потрібно реагувати. На стратегічний вибір впливають: ризик, на який готова йти фірма; досвід реалізації чинних стратегій, позиції власників, наявність часу. Розглянемо особливості стратегічних рішень. За ступенем регламентованості вони належать до контурних (надають широку свободу виконавцям стосовно тактики), а за ступенем обов'язковості проходження головним установкам – директивним.

За функціональним призначенням такі рішення найчастіше бувають організаційними або розпорядчими способами здійснення в певних ситуаціях тих чи інших дій. З точки зору визначеності, це рішення запрограмовані. Вони приймаються в нових, неординарних обставинах, коли необхідні кроки важко заздалегідь точно розписати. З точки зору важливості, стратегічні рішення кардинальні: стосуються основних проблем і напрямків діяльності фірми, визначають основні шляхи розвитку її в цілому, окремих підрозділів або видів діяльності на тривалу перспективу (не менше 5–10 років). Вони випливають насамперед із зовнішніх, а не з внутрішніх умов, повинні враховувати тенденції розвитку ситуації і інтереси безлічі суб'єктів. Практична незворотність стратегічних рішень обумовлює необхідність їх ретельної та всебічної підготовки. Стратегічним рішенням притаманна комплексність. Стратегія зазвичай являє собою не одне, а сукупність взаємопов'язаних рішень, об'єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсами.

Такі рішення визначають пріоритети і напрямки розвитку фірми, її потенціалу, ринків, способи реакції на непередбачені події. Практика сформувала нижченаведені вимоги до стратегічних рішень:

1. Реальність, що передбачає її відповідність ситуації, цілям, технічному та економічному потенціалу підприємства, досвіду і навичками працівників і менеджерів, культурі, існуючій системі управління;

2. Логічність, зрозумілість, прийнятність для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

3. Своєчасність (реалізація рішення повинна встигнути призупинити негативне розвиток ситуації або не дозволити упустити вигоду);

4. Сумісність із середовищем, що забезпечує можливість взаємодії з нею (стратегія перебуває під впливом змін в оточенні підприємства і сама може формувати ці зміни);

5. Спрямованість на формування конкурентних переваг;

6. Збереження свободи тактичного маневру;

7. Усунення причин, а не наслідків існуючої проблеми;

8. Чіткий розподіл за рівнями організації роботи з підготовки та прийняття рішень, а також відповідальності за них конкретних осіб;

9. Облік прихованих і явних, бажаних і небажаних наслідків, які можуть виникнути при реалізації стратегії або відмову від неї для фірми, її партнерів; в зв'язку з існуючим законодавством, етичною стороною справа, допустимим рівнем ризику та інше. Розробка науково обґрунтованої системи стратегій організації як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

– виділяти, відстежувати і оцінювати ключові проблеми;

– адекватно і оперативно реагувати на зміни всередині і в оточенні організації;

– вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;

– створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу. Вихідний момент формування стратегії – постановка глобальних якісних цілей і

параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув'язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінювання яких дозволяє вибрати кращу стратегію. Єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід. Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці безлічі стратегій захисту, і вибір такого мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах. Відповідно до найбільш реальних варіантів поєднань значень розглянутих факторів виділено три стратегії захисту:

– оборонна – захист від вже відомих загроз здійснюваний автономно, тобто без надання істотного впливу на інформаційно - керувальну систему;

– наступальна – захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно - керувальної системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;

– упереджувальна – створення інформаційного середовища, в якому загрози інформації не мали б умов для прояву.

3.2 Побудова захисту інформаціїї

Під системою захисту КС розуміють єдину сукупність правових і морально-етичних норм, адміністративно-організаційних мір, фізичних і програмно-технічних засобів, спрямованих на протидію погрозам КС з метою зведення до мінімуму можливості збитку. Процес побудови системи захисту включає наступні етапи:

- аналіз можливих погроз КС;
- планування системи захисту;
- реалізація системи захисту;

- супровід системи захисту.

Етап аналізу можливих погроз КС необхідний для фіксації стану АСОІ – визначення конфігурації апаратних і програмних засобів, технології обробки інформації і виявлення впливів, що діють на компоненти системи. Практично неможливо забезпечити захист АСОІ від усіх впливів, оскільки неможливо цілком установити всі погрози і способи їхніх реалізацій. Тому з усієї множини ймовірних впливів вибирають тільки такі впливи, що можуть реально відбутися і завдати серйозної шкоди. На етапі планування формулюється система захисту як єдина сукупність мір протидії погрозам різної природи . За способами здійснення всі міри забезпечення безпеки комп'ютерних систем підрозділяють на:

1. Нормативно-правові (законодавчі). 2. Морально-етичні. 3. Адміністративні (організаційні). 4. Фізичні (технічні). 5. Апаратно-програмні. Перераховані міри безпеки КС можна розглядати як послідовність бар’єрів або рубежів захисту інформації. Для того щоб добратися до інформації, що захищається, потрібно послідовно перебороти кілька рубежів захисту. Розглянемо їх докладніше. Перший рубіж захисту, що встає на шляху людини, яка намагається здійснити НСД до інформації, є правовим. Цей аспект захисту інформації зв'язаний з необхідністю дотримання юридичних норм при передачі й обробці інформації.

До правових мір захисту інформації відносяться діючі в країні закони, укази й інші нормативні акти, що регламентують правила роботи з інформацією обмеженого використання і відповідальності за їхні порушення. Цим вони перешкоджають несанкціонованому використанню інформації і є стримуючим чинником для потенційних порушників. Другий рубіж захисту утворюють морально-етичні міри. Етичний момент у дотриманні вимог захисту має досить велике значення. Дуже важливо, щоб люди, що мають доступ до комп’ютерів, працювали в здоровому моральноетичному кліматі.

До морально-етичних мір протидії відносяться норми поводження, що традиційно склалися або складаються в суспільстві в міру поширення комп’ютерів у країні. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені, але їхнє недотримання звичайне веде до падіння престижу людини, групи осіб або організації. Морально-етичні норми бувають як неписаними (наприклад, загальновизнані норми чесності, патріотизму і т.д.), так і оформленими в якийсь звід правил або розпоряджень. Адміністративні міри захисту відносяться до мір організаційного характеру. Вони регламентують:

- процеси функціонування КС;
- використання ресурсів КС;
- діяльність її персоналу;
- порядок взаємодії користувачів із системою, для того щоб найбільшою мірою утруднити або виключити можливість реалізації погроз безпеки. Адміністративні міри включають:
- розробку правил обробки інформації в КС;
- сукупність дій при проектуванні й устаткуванні обчислювальних центрів і інших об'єктів КС (облік впливу стихії, пожеж, охорона приміщень);
- сукупність дій при підборі і підготовці персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки; створення умов, при яких персоналові було б невигідно припускатися зловживань і т.д.);
- організацію надійного пропускного режиму;
- організацію обліку, збереження, використання і знищення документів і носіїв з конфіденційною інформацією;
- розподіл реквізитів розмежування доступу (паролів, повноважень і т.п.);

• організацію схованого контролю за роботою користувачів і персоналу КС;

• сукупність дій при проектуванні, розробці, ремонті і модифікації устаткування і програмного забезпечення (сертифікація використовуваних технічних і програмних засобів, строге санкціонування, розгляд і твердження всіх змін, перевірка на задоволення вимогам захисту, документальна фіксація змін і т.д.). Важливо відзначити, що, поки не будуть реалізовані дійові заходи адміністративного захисту ЕОМ, інші міри будуть, безсумнівно, неефективні.

Адміністративно-організаційні міри захисту можуть здатися нудними і рутинними в порівнянні з морально-етичними і позбавленими конкретності в порівнянні з апаратно-програмними. Однак вони являють собою могутній бар'єр на шляху незаконного використання інформації і надійну базу для інших рівнів захисту. Четвертим рубежем є фізичні міри захисту. До фізичних мір захисту відносяться різного роду механічні, электро- і електронно-механічні пристрої або спорудження, спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи й інформації, що захищається. П'ятим рубежем є апаратно-програмні засоби захисту. До них відносяться різні електронні пристрої і спеціальні програми, що реалізують самостійно або в комплексі з іншими засобами наступні способи захисту: ідентифікацію (розпізнавання) і аутентифікацію (перевірка дійсності) суб'єктів (користувачів, процесів) КС; розмежування доступу до ресурсів КС; контроль цілісності даних; забезпечення конфіденційності даних; реєстрацію й аналіз подій, що відбуваються в КС; резервування ресурсів і компонентів КС.

3.3 Основні принципи організації КСЗІ

Захист інформації в автоматизованих системах овинен ґрунтуватися на таких основних принципах:

• системності;

• комплексності;

• безперервності захисту;

• розумної достатності;

• гнучкості управління і застосування;

• відкритості алгоритмів і механізмів захисту;

• простоти застосування захисних заходів і засобів.

3.3.1 Принцип системності

Системний підхід до захисту комп'ютерних систем передбачає необхідність врахування всіх взаємозв'язаних, взаємодійних і змінних в часі елементів, умов та факторів, істотно значущих для розуміння і вирішення проблеми забезпечення безпеки АЕС. При створенні системи захисту необхідно враховувати всі слабкі, найбільш вразливі місця системи обробки інформації, а також характер, можливі об'єкти і напрямки атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в розподілені системи і НСД до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення і НСД до інформації, але й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеці.

3.3.2 Принцип комплексності

У розпорядженні фахівців з комп'ютерної безпеки є широкий спектр заходів, методів і засобів захисту комп'ютерних систем. Комплексне їх використання передбачає узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі істотні канали реалізації загроз і не містить слабких місць на стиках окремих її компонентів. Захист повинен будуватися ешелоновано. Зовнішній захист повинен забезпечуватися фізичними засобами, організаційними та правовими заходами. Однією з найбільш укріплених ліній оборони покликані бути засоби захисту, реалізовані на рівні операційних систем (ОС) в силу того, що ОС – це якраз та частина

комп'ютерної системи, яка керує використанням всіх її ресурсів. Прикладний рівень захисту, що враховує особливості предметної області, є внутрішнім рубежем оборони.

3.3.3 Принцип безперервності захисту

Захист інформації – це не разовий захід і навіть не певна сукупність проведених заходів та встановлених засобів захисту, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу АС, починаючи з найперших стадій проектування, а не тільки на етапі її експлуатації. Розробка системи захисту повинна вестися паралельно з розробкою самої захищуваної системи. Це дозволить врахувати вимоги безпеки при проектуванні архітектури і, в підсумку, дозволить створити більш ефективні (як за витратами ресурсів, так і за стійкістю) захищені системи. Більшості фізичних і технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна організаційна (адміністративна) підтримка (своєчасна зміна та забезпечення правильного зберігання і застосування імен, паролів, ключів шифрування, перевищення повноважень тощо). Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу застосовуваних методів і засобів захисту, для впровадження спеціальних програмних і апаратних «закладок» й інших засобів подолання системи захисту після відновлення її функціонування.

3.3.5 Розумна достатність

Створити абсолютно неперебрну систему захисту принципово неможливо. При достатній кількості часу і коштів можна подолати будьякий захист. Тому має сенс вести мову тільки про деякий прийнятний рівень безпеки. Високоефективна система захисту коштує дорого, використовує при роботі істотну частину потужності й ресурсів комп'ютерної системи і може створювати відчутні додаткові незручності користувачам. Важливо правильно вибрати той достатній рівень захисту, при якому витрати, ризик і розмір можливого збитку були б прийнятними (задача аналізу ризику).

3.3.6 Гнучкість системи захисту

Часто доводиться створювати систему захисту в умовах великої невизначеності. Тому вжиті заходи та встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнем захищеності засоби захисту повинні мати певну гнучкість. Особливо важливою ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснювати на систему, що працює, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з плином часу змінюються. У таких ситуаціях властивість гнучкості рятує власників АС від необхідності вживання кардинальних заходів з повної заміни засобів захисту на нові.

3.3.7 Відкритість алгоритмів і механізмів захисту

Суть принципу відкритості алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок обмеження доступу до структурної організації та алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно давати можливості її подолання (навіть авторові). Однак це зовсім не означає, що інформація про конкретну систему захисту повинна бути загальнодоступною.

3.3.8 Принцип простоти застосування засобів захисту

Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових трудовитрат при звичайній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (введення декількох паролів та імен і т. д.).

3.4 Захист за допомогою брандмауерів.

При підключенні мережі організації до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів щодо захисту студії веб-

дизайну. При побудові захисту слід виходити з того, що будь-який захист ускладнює використання системи, яка захищається, за прямим призначенням обмежує функціональні можливості, використовує обчислювальні і трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вищий захист, тим більш дорогою у створенні та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів. Тому, захищаючи мережу, слід виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсу, що захищається. Існує ряд основних принципів, що дозволяють організувати досить безпечне підключення до мережі Інтернет порівняно простими засобами. Мабуть, основним загальновизнаним засобом такого захисту є міжмережевий екран (брандмауер). Міжмережевий екран встановлюється між мережею, що захищається, і мережею Інтернет, і виконує роль мережевого фільтра. Він настроюється так, щоб пропускати допустимий трафік від користувачів мережі, що захищається, до служб Інтернет і назад, і обмежити трафік з боку Інтернет у мережу, що захищається тільки необхідними службами, наприклад: smtp, dns, ntp. Допустимість того або іншого трафіку визначається мережевим адміністратором відповідно до політики інформаційної безпеки організації.

Наприклад, може бути дозволений доступ з частини комп'ютерів мережі, що захищається, до web і ftp-серверів Інтернет і двонаправлений доступ між Інтернет і поштовим сервером мережі, що захищається, але заборонені всі інші протоколи і напрями трафіку. З огляду на те, що міжмережевий екран фізично розташовується на місці мережевого шлюзу (маршрутизатора), логічно є доцільним об’єднати їх функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і, безпосередньо, сам шлюз. Така опція передбачена для маршрутизаторів компанії Cisco Systems (називається Firewall Feature Set). Проте дане правило є необов'язковим і міжмережевий екран може бути подано окремим пристроєм.

У простому випадку виконання функцій міжмережевого екрана можна організувати за допомогою мережевого фільтра на основі листів доступу

(access-lists). Листи доступу визначають правила, за якими дозволяється або забороняється проходження трафіку з певними ознаками від одного мережевого інтерфейсу маршрутизатора до іншого усередині самого маршрутизатора. IP-адреса або діапазон IP-адрес джерела і приймача, тип протоколу, номер порту призначення або відправлення, ряд інших службових ознак IP-пакета можуть використовуватися як ознаки (рис. 3.1). Відмінність і недолік листів доступу в порівнянні зі справжнім міжмережевим екраном полягає в тому, що вони дозволяють створити статичний односторонній фільтр, тоді як мережеве з'єднання є динамічним процесом. Листи доступу не дозволяють контролювати параметри IP-пакета, залежні від попередніх пакетів. Звідси виникає складність застосування листів доступу для тонкої настройки фільтрації трафіку в точній відповідності з прийнятою політикою безпеки. Зокрема, з цієї причини листи доступу не в змозі захистити від такого різновиду мережевої атаки, як “крадіжка з'єднання” або “хай-джекинг”.

У Firewall Feature Set указані проблеми розв'язуються за допомогою того, що він відстежує кожне мережеве з'єднання окремо і контролює весь процес у динаміці. При встановленні нового TCP-сеансу міжмережевий екран створює для нього новий процес, який контролює правильність з'єднання до самого моменту його завершення. При цьому кожен пакет, що приходить на транспортному рівні, перевіряється на відповідність попередньому, а всі “підозрілі” пакети вибраковуються. Таким чином, стає можливим застосування фільтра доступу внутрішнього комп'ютера до зовнішньої мережі, що не дозволяє зовнішньому комп'ютеру самостійно звернутися до внутрішнього. Іншими словами, в налаштуваннях міжмережевого екрана задаються правила для проходження трафіку від одного інтерфейсу до іншого, для кожного напряму і кожного тракту окремо. Якщо правило вирішує проходження IP-пакета від інтерфейсу внутрішньої мережі до Інтернет - інтерфейсу, то на підставі такого пакета формується логічний тунель у маршрутизаторі, через який вже можуть пройти у відповідь пакети від зовнішнього одержувача. Як тільки з'єднання переривається або вичерпується час очікування, тунель закривається, і звернення

ззовні до внутрішнього комп'ютера будуть виключені. З цієї ж причини екран не пропустить пакети у зворотному напрямку, якщо ініціатором з'єднання є зовнішній комп'ютер. Крім того, міжмережевий екран, на відміну від листів доступу, може контролювати зміст IP-пакетів у полі даних і відбраковувати пакети, що містять потенційнонебезпечні коди, наприклад java-аплети. Існують міжмережеві екрани, здатні виявити в IP-пакетах ознаки відомих мережевих атак і перервати таке з'єднання, але це вже достатньо дорогі системи. Другою цеглинкою забезпечення захищеності мережі є “заміна мережевої адреси” – (Network Address Translation), або NAT. Це заміна в IP-пакеті реальної адреси комп'ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні її до зовнішньої мережі. Таким чином, для внутрішньої мережі стає можливим використання діапазонів адрес, які не вживаються в мережі Інтернет (10.0.0.0-10.255.255.255)

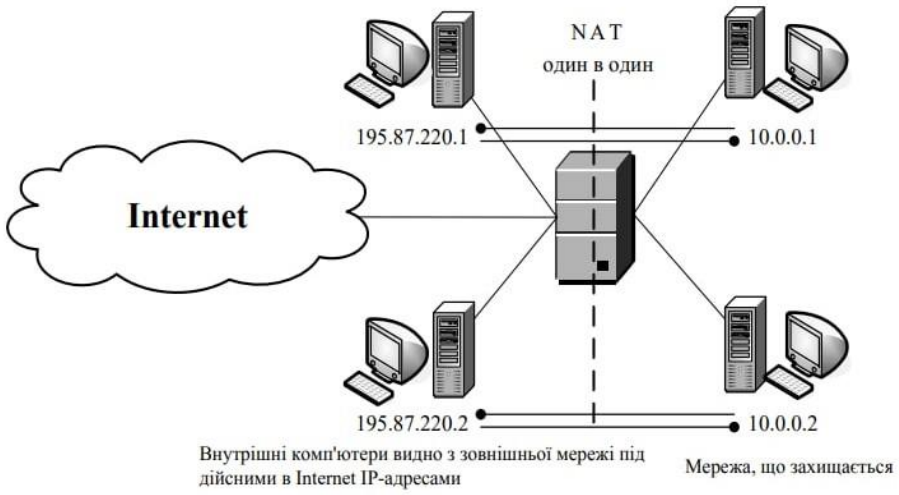

Рис. 3.1 Приклад побудови мережі на основі листів доступу

Найбільш простою і найбільш дешевою з точки зору захисту є трансляція фіксованої внутрішньої адреси у фіксованій зовнішній. При цьому зловмисник безперешкодно “бачить” такий комп'ютер в зовнішній мережі, оскільки йому однозначно відповідає певна зовнішня адреса. Проте вона необхідна при організації сервера, до якого потрібно забезпечити доступ ззовні.

Друга форма NAT – це трансляція групи внутрішніх адрес до однієї зовнішньої.

При цьому всі внутрішні комп'ютери можуть працювати з мережею Інтернет одночасно, а маршрутизатор розрізняє, кому яку відповідь перетранслювати за службовими даними TCP-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Така заміна істотно ускладнює життя зловмиснику, оскільки повністю приховує внутрішні комп'ютери і перешкоджає “вирахуванню” жертви. Зловмисник, навіть побачивши звернення, що випливають з внутрішньої мережі, не зможе визначити, з якого комп'ютера вони виходять.

Демілітаризована зона. Як правило, організації потрібно мати у себе деякі мережеві ресурси, до яких відкрито доступ з мережі Інтернет. Зазвичай це поштовий, dns-і web-сервери. Механізм їх роботи припускає можливість вільного або майже необмеженого звернення з мережі Інтернет. Відповідно, ймовірність їх зламу вища, ніж решти комп'ютерів мережі.Рис. 3.2 Приклад побудови мережі з використанням для заміни внутрішніх адрес пулу виділених адрес. Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережевим екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну зону їх розміщення називають “демілітаризованою зоною” (рис. 3.2).

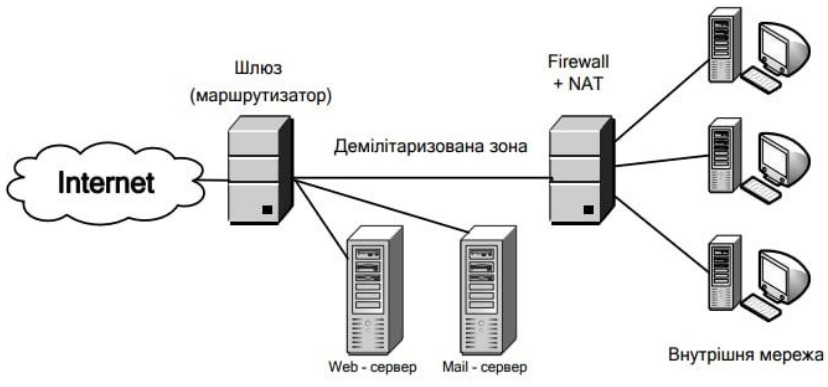

Рис. 3.2 Приклад побудови мережі з демілітаризованою зоною

З рис. 3.3 видно, що ніщо не заважає встановити другий Firewall на основному шлюзі мережі. Це є логічним рішенням і дозволяє одночасно

підвищити рівень захисту внутрішньої мережі і захистити сервери демілітаризованої зони. При правильному налагодженні обох міжмережевих екранів зловмиснику буде вже набагато важче дістатися до внутрішньої мережі організації.

Наявність другого міжмережевого екрана (рис 3.3) дещо ускладнює конфігурацію мережевого устаткування і настройку роботи всіх елементів мережі. Для додаткового підвищення захищеності можна використовувати Firewall'и різних виробників. Тоді, якщо в одному з них буде виявлено уразливість, інший не дозволить зловмиснику безперешкодно проникнути до мережі, як це мало б місце при використанні Firewall'ов одного типу.

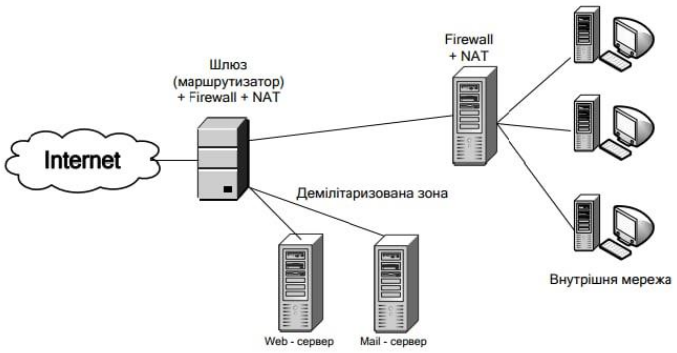

Рис. 3.3 Приклад побудови мережі з другим Firewall'ом (брандмауером)

Тут слід особливо підкреслити, що для унеможливлення зловмисного втручання мережевий доступ до шлюзів і міжмережевих екранів має бути відключений. З погляду безпеки пристрої, що охороняють мережу, повинні конфігуруватися і адмініструватися тільки через консольний порт локально.

Використання proxy-сервера також підвищує рівень захищеності мережі, оскільки виключає необхідність прямого виходу в Інтернет комп'ютерівкористувачів. При цьому також стає можливим більш суворий контроль за даними в IP-пакетах на рівні мережевих додатків. Proxy-сервер працює як посередник між призначеним для користувача додатком і віддаленим мережевим ресурсом до Інтернет. Принцип його роботи схематично показано на рис. 3.4

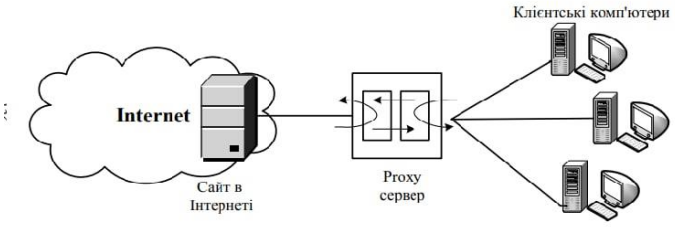

Рис. 3.4 Приклад побудови мережі з proxy-сервером

Proxy-сервер складається з двох частин: клієнтської і серверної. Клієнтська частина дивиться у бік Інтернет, серверна – у бік клієнтського комп'ютера. Коли клієнтський комп'ютер звертається до віддаленого сайту через proxy-сервер, його клієнтський мережевий додаток взаємодіє з серверною частиною proxy-сервера.

4. Розробка комплексних систем захисту інформації студії Web-дизайну

Комплексна система захисту інформації студії Web-дизайну наведена нас (рис.4.1) Основне завдання КСЗІСВД полягає в блокуванні технічних каналів витоку інформації та ліквідації наслідків реалізації загроз інформації. Загрози інформації складаються з багатьох факторів, тому завдання захисту потребує комплексного підходу з використанням новітніх технічних засобів і наукових розробок. Вирішення завдань включають в себе аналіз об'єкта захисту, розробку системи виявлення каналів витоку інформації та економічне обґрунтування необхідності використання системи захисту інформації.

Рис. 4.1 Розроблена схема комплексної системи захисту інформації студії Web-дизайну

КСЗІСВД являє собою діючі у єдиній сукупності законодавчі, організаційні, технічні, криптографічні та інші заходи і засоби, які забезпечують

захист інформації студії Web-дизайну від усіх визначених загроз і можливих каналів її витоку, і особливо каналів електромагнітного випромінювання.

На сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки студії Web-дизайну, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень інформаційної безпеки впливає на розвиток та впровадження науково-технічних інновацій у процеси виробництва, збереження стабільності функціонування можливості економічного зростання.

Структура засобів КСЗІ зображена на рис. 4.2. Організаційно-правовими заходами реалізується комплекс відповідній нормативно-правовій базі держави адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності і засобів ТЗІ, а також шляхом створення служб, відповідальних за їх реалізацію. Основним завданням технічних заходів є забезпечення фізичної інформаційної безпеки. Фізичні заходи захисту інформації створюють пристрої та споруди, проводять заходи, що утруднюють або унеможливлюють проникнення потенційних порушників у місця, де можна мати доступ до системи управління та інформації, що захищається.

Пропонується застосувати фізичну ізоляцію споруди, де встановлена апаратура, від інших будівель зокрема – огородження й систематичний контроль території, організація контрольно-пропускних пунктів, обладнання вхідних дверей спеціальними замками, організація системи охоронної сигналізації.

У робочий час, коли ПК працює, можливий витік інформації каналами побічного електромагнітного випромінювання. Для усунення такої загрози здійснюються спеціальні дослідження щодо апаратих засобів та їх випромінювання, основним змістом яких є атестування та категорування засобів і об'єктів електронно-обчислювальної техніки (ЕОТ) з видачею відповідного дозволу на експлуатацію. Крім того, двері приміщення повинні бути обладнані механічним або електромеханічним замком. У деяких випадках, коли відсутня

охоронна сигналізація, на період тривалої відсутності користувача ПК для підвищення безпеки доцільно системний блок і машинні носії інформації зберігати в сейфі. Використання в деяких ЕОМ у системі вводу-виводу BIOS апаратного паролю, що блокує завантаження і роботу ПК, не зовсім надійно забезпечує захист від загроз НСД, оскільки при відсутності на корпусі системного блоку механічного замка та самого власника-користувача апаратна частка BIOS-носія паролю може бути замінена на іншу таку ж, оскільки вузли BIOS уніфіковані, але вже з відомим значенням паролю. Саме тому механічний замок, що блокує вмикання і завантаження ПК, найбільш ефективний захід у цьому випадку.

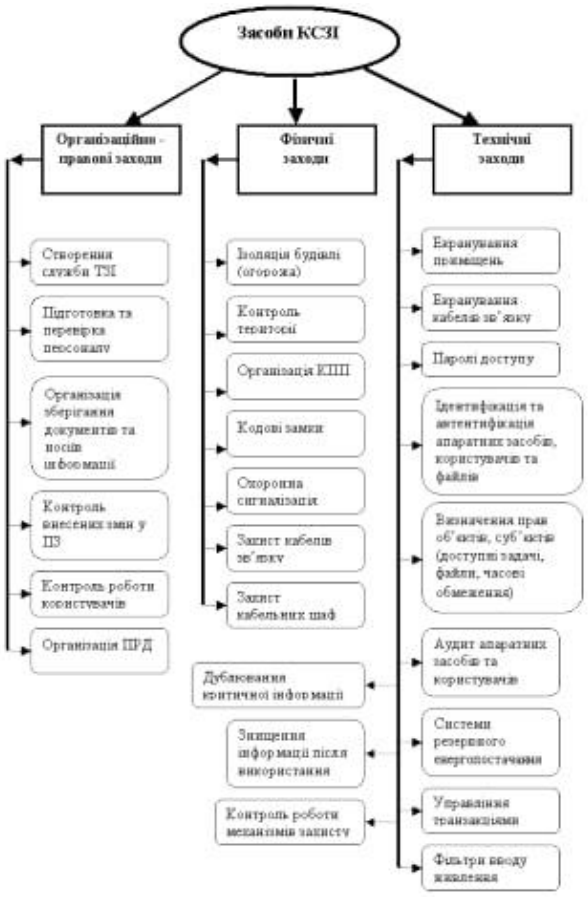

Рис. 4.2 Структура засобів КСЗІ

Інформаційна система(ІС) підприемства є технічно-організаційною системою, в нії реалізуються інформаційні системи, це зумовлює використання,

програмно-апаратного та інших видів забезпечення, потрібного для реалізації документальних процесів збору, копіювання, обробки, передачі, зберігання, пошуку і розповсюдження данних. Основу сучасної інформаційної системі підприемства, як правило, складають глобально розподілені КС (обчислювальні мережі) які розташовані в різних будівлях, на окремих поверхах і з'єднані між собою транспортним середовищем, яке використовує фізичні принципи з'єднання між зобою за допомогою: "витої парі", оптико-волоконних каналів, радіоканалів та іншими способами. Основу технічних пристроїв таких систем становлять електронні обчислювальні машини, периферійні, допоміжні пристрої та пристрої зв'язку, що з'єднані з ЕОМ. Склад програм визначається можливостями електронно обчислювальної машини і характером вирішуваних завдань в даній ІС. Систему складають такі елементі як: - безпосередньо користувачі. - окремі ПК і робочі станції; - робоче місце віддаленого користувача; - робочі місця співробітників ІС; - канали і засоби зв'язку (КЗ); - локальна мережа; - виробничі лабораторії; - носії інформації (магнітні, оптичні і ін.); Названі елементи в процесі співпраці, активно взаємодіють між собою, що дозволяє застосовувати різні точки доступу до ресурсів данних: це архів, комп'ютерні кабінети, Інтернет-кафе, система доступу працівників з домашніх комп'ютерів, відомих як: «хмарні технології». Як результат постійного зростання кількості злочинів у сфері безпеки інформації постійно з'являються нові вимоги до захисту баз інформаційних даних студії веб-дизайну та виникає потреба у розробці власної інтегрованої системи безпеки. Вона задає наявність нормативно-правової бази, формування концепції безпеки, розробку власних заходів, етапів і процедур щодо безпеки під час роботи, проектування, реалізації і супровід технічних засобів захисту бази інформації що обробляється на підприємстві.

Звідси виникає необхідність в визначенні єдиної політики забезпечення безпеки інформації на підприємстві. Роботи по кожному з названих елементів відіграють фрагментарний характер і пов'язано це з: - неповним фінансуванням запланованих робіт із захисту інформації; - відсутністю єдиної політики безпеки

інформації підприємств; - відсутність у керівників та працівників чітких уявлень про те, що саме і як необхідно захищати. Тільки комплексна робота усіх процесів управління безпекою інформаційних даних підприємства може створити безпечне інформаційне середовище.

Економічна частина

Метою даних розрахунків є обчислення вартості виконання науково-дослідної роботи « Розробка комплексних заходів безпеки інформаційних систем студії веб-дизайну». Основна мета даного дипломного проекту є своєчасне виявлення загроз та запобігання порушенню цілісності інформації з обмеженим доступом і витоку її технічними каналами.

Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення. Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців.. Розподіл робіт по етапах і видах виконавців вироблений формою, наведено в таблиці 4.1.

Розподіл робіт по етапах і видах виконавців.

Таблиця 4.1.

Етап проведення НДР	**Вигляд робіт**	**Посада виконавця**
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР «Розробка комплексних заходів безпеки інформаційних систем студії веб-дизайну»	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури. 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР .	Дипломник керівник

	3. Вибір напряму проведення досліджень для подальшої розробки. 4. Розробка плану проведення досліджень для подальшої розробки.	
Теоретичні і експериментальні дослідження	Інформаційні системи студії веб-дизайну Інформаційна безпека Комплексна система захисту інформації	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів попередніх етапів роботи. 2. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому.	Дипломник керівник консультанти

В умовах відсутності нормативної бази тривалість виконання окремих робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Очікувана трудомісткість робіт.

Таблиця 4.2.

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР « Розробка комплексних заходів безпеки інформаційних систем студії веб-дизайну »	**1**
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	**6**
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	**2**
4. Вибір напряму проведення досліджень і способів вирішення поставлених завдань. Розробка плану проведення досліджень для	**2**

подальшої розробки.	
5. Огляд технології захисту комп'ютерних систем	**5**
6. Програмні засоби інформаційної системи студії веб-дизайну	**3**
7. Програмне забезпечення студії веб-дизайна	**1**
8 Основні принципи організації КЗСІ	**2**
Всього:	**22**

Результатом виконання НДР є науково-технічна продукція, що є закінчені науково – дослідницькі роботи, виконані відповідно до вимог, передбачених договором, і прийнятими замовником. Розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали, купувальні комплектуючі, напівфабрикати визначають на основі розрахунку потреби в них за оптовими цінами, що діють і складають (70 + 140) 210 грн.

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2022» встановлено мінімальну заробітну плату у місячному розмірі з 1 січня 2022 року - 6500 гривень; мінімальну погодинну тарифну ставку – 39,26 грн.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

$$Зден= п.т.с. * 8;$$

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня,год.

Зден дипломника = 39.26*8 = 314,08 грн.

Зден керівника 65*8 = 520 грн.

Зден консультантів = 60*8= 480грн.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 5.3.

Витрати на основну заробітну плату.

Таблиця 4.3.

Виконавець	**Погодинна тарифна ставка, грн**	**Денна ставка, грн**	**Трудомісткість робочих днів**	**Сума основної зарплати, грн**
Дипломник	39,26	314.08	22	6909,76
Керівник	65	520	1	520
Консультант по економічній частині	60	480	0,25	60,25
Консультант по охороні праці	60	480	0,25	60,25
Нормоконтроль	60	480	0,25	60,25
Всього (Зо)				7610,51

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної і враховують виплати за час, що не пропрацював, встановлений законом. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

$$Зд=10\%Зо;$$

$$Зд= 7610,51*0,12=913,26 \text{ грн}$$

4)До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає.

Зєсв=0,22*(Зо+Зд);

Зєсв= 0,22*(7610,51+913,26)=8524,11*0,22=1875,30 грн

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР.. У наукових закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

Рнакл= (Зо+Зд)*0,4;

Рнакл= (7610,51+913,26)*0,3=2557,23 грн

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 5.4.

Калькуляція планової собівартості

Таблиця 4.4.

Статті витрат	Сума, грн.
1. Матеріали	210
2. Основна заробітна плата	7610,51
3. Додаткова заробітна плата	913,26
4. Відрахування до єдиного соціального внеску	1875,30
5. Накладні витрати	2557,23
Планова собівартість (Спл)	13166,3

Плановий прибуток визначений по формулі:

Ппл = 0,1*13166,3= 1316,63грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Договірна ціна визначається по формулі:

Цнір = 13166,3 + 1316,63 = 14482,93грн

Звідси ціна реалізації становить:

Цр = 14482,93 + 2896,58= 14482,93+ 14482,93*0,2

Цр = 17373,51грн.

Охорона праці

Вступ

Охорона здоров'я працюючих, забезпечення безпеки умов праці, ліквідація професійних захворювань і виробничого травматизму складає одну з головних турбот людського суспільства. Звертається увага на необхідність широкого застосування прогресивних форм наукової організації праці, зведення до мінімуму ручної, малокваліфікованої праці, створення обстановки, що виключає професійні захворювання і виробничий травматизм.

На робочому місці повинні бути передбачені заходи захисту від можливого впливу небезпечних і шкідливих факторів виробництва. Рівні цих чинників не повинні перевищувати граничних значень, обумовлених правовими, технічними та санітарно-технічними нормами. Ці нормативні документи зобов'язують до створення на робочому місці умов праці, при яких вплив небезпечних і шкідливих чинників на працюючих або усунуто зовсім, або знаходиться в допустимих межах.

2. Характеристика умов праці програміста та можливих шкідливих та небезпечних виробничих чинників

Науково-технічний прогрес вніс серйозні зміни в умови виробничої діяльності робітників розумової праці. Їх праця стала більш інтенсивним, напруженим, які вимагають значних витрат розумової, емоційної і фізичної енергії

При роботі з комп'ютером людина піддається дії ряду небезпечних і шкідливих виробничих факторів: електромагнітних полів (діапазон радіочастот), інфрачервоного і іонізуючого випромінювань, шуму і вібрації, статичної електрики і ін.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ЕОМ. Велике значення має раціональна конструкція і розташування

елементів робочого місця, що важливо для підтримки оптимальної робочої пози людини-оператора.

У процесі роботи з комп'ютером необхідно дотримувати правильний режим праці та відпочинку.

3 Розробка заходів з охорони праці

2.1 Виробничі приміщення

Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше 6,0 м^2, а об'єм – не менше ніж 20,0 м^3. У приміщеннях слід щоденно робити вологе прибирання. Вони повинні бути оснащені аптечками першої медичної допомоги. При приміщеннях мають бути обладнанні побутові приміщення для відпочинку.

Виробниче середовище.

2.3 Мікроклімат робочої зони працівників, вентиляція.

Принцип нормування мікроклімату - створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Комп'ютерна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вологості в приміщенні. У приміщеннях, де встановлені комп'ютери, повинні дотримуватися певні параметри мікроклімату.

У санітарних нормах СН-245-71 встановлені величини параметрів мікроклімату, що створюють комфортні умови. Ці норми встановлюються в залежності від пори року, характеру трудового процесу і характеру виробничого приміщення

Таблиця 1 Параметри мікроклімату для приміщень, де встановлені комп'ютери

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні Відносна вологість Швидкість руху повітря	22 ... 24 ° С 40 ... 60%

		до 0,1 м / с
Теплий	Температура повітря в приміщенні Відносна вологість Швидкість руху повітря	23 ... 25 ° С 40 ... 60% 0,1 ... 0,2 м / с

2.2 Освітлення робочого місця, шум, вібрація

Недостатність освітлення приводить до напруги зору, ослабляє увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає засліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань, тому такий важливий правильний розрахунок освітленості.

Вимоги до освітленості в приміщеннях, де встановлені комп'ютери, наступні: при виконанні зорових робіт високої точності загальна освітленість повинна складати 300лк, а комбінована - 750лк; аналогічні вимоги при виконанні робіт середньої точності - 200 і 300лк відповідно.

Згідно СНіП II-4-79 в приміщень необхідно застосувати систему комбінованого освітлення. Комбіноване - освітлення, при якому до загального додається місцеве освітлення.

В якості джерел штучного освітлення звичайно використовуються люмінесцентні лампи типа ЛБ, або ДРЛ, які попарно об'єднуються в світильники, які повинні розташовуватися рівномірно над робочими поверхнями.

Вимоги до освітленості в приміщеннях, де встановлені комп'ютери, наступні: при виконанні зорових робіт високої точності загальна освітленість повинна складати 300лк, а комбінована - 750лк; аналогічні вимоги при виконанні робіт середньої точності - 200 і 300лк відповідно.

Джерела світла, такі як світильники і вікна, які дають віддзеркалення від поверхні екрану, значно погіршують точність знаків і тягнуть за собою

перешкоди фізіологічного характеру, які можуть виразитися в значній напрузі, особливо при тривалій роботі. Для захисту від надмірної яскравості вікон можуть бути застосовані штори і екрани.

Крім того все поле зору повинне бути освітлено достатньо рівномірно - ця основна гігієнічна вимога. Іншими словами, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими, оскільки яскраве світло в районі периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності.

Рівень шуму на робочому місці математиків-програмістів і операторів відеоматеріалів не повинен перевищувати 50дБА, а в залах обробки інформації на обчислювальних машинах - 65дБА. Для зниження рівня шуму стіни і стеля приміщень, де встановлені комп'ютери, можуть бути облицьовані звукопоглинальними матеріалами. Рівень вібрації в приміщеннях обчислювальних центрів може бути понижений шляхом встановлення устаткування на спеціальні віброізолятори.

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітора комп'ютера представлені в табл. 3.4.

Таблиця 2 Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50см від поверхні відеомонітора	10В / м
Напруженість магнітної складової електромагнітного поля на відстані 50см від поверхні відеомонітора	0,3 А / м
Напруженість електростатичного поля не повинна	

перевищувати: для дорослих користувачів для дітей дошкільних установ і що вчаться середніх спеціальних і вищих навчальних закладів	20кВ / м 15кВ / м

Для зниження дії цих видів випромінювання рекомендується застосовувати монітори із зниженим рівнем випромінювання (MPR-II, TCO-92, TCO-99), встановлювати захисні екрани, а також дотримуватися регламентовані режими праці та відпочинку.

2.4 Організація робочого місця користувача ПК

Робоче місце і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи.

Головними елементами робочого місця програміста є стіл і крісло. Основним робочим положенням є положення сидячи.Велике значення надається характеристикам робочого крісла. Так, рекомендована висота сидіння над рівнем підлоги перебуває в межах 420-550мм. Поверхня сидіння м'яка, передній край закруглений, а кут нахилу спинки - регульований.

Робоча поза сидячи викликає мінімальне стомлення програміста. Раціональне планування робочого місця передбачає чіткий порядок і сталість розміщення предметів, засобів праці і документації. Те, що потрібно для виконання робіт частіше, розташоване в зоні легкої досяжності робочого простору.Причина неправильної пози користувачів обумовлена наступними чинниками: немає хорошої підставки для документів, клавіатура знаходиться дуже високо, а документи - низько, нікуди покласти руки і кисті, недостатній простір для ніг.

Оптимальне розміщення предметів праці і документації в зонах досяжності:

- ДИСПЛЕЙ розміщається в зоні а (у центрі);
- СИСТЕМНИЙ БЛОК розміщається в передбаченій ніші столу;
- КЛАВИАТУРА - у зоні г / д;
- «МИША» - в зоні в справа;
- СКАНЕР в зоні а / б (зліва);
- ПРИНТЕР знаходиться в зоні а (праворуч);
- ДОКУМЕНТАЦІЯ: необхідна при роботі - в зоні легкої досяжності долоні - в, а у висувних ящиках столу - література, невикористовувана постійно.

Під час користування комп'ютером медики радять встановлювати монітор на відстані 50-60 см від очей. Фахівці також вважають, що верхня частина відеодисплея повинна бути на рівні очей або трохи нижче.

З метою подолання вказаних недоліків даються загальні рекомендації: краще пересувна клавіатура; повинні бути передбачені спеціальні пристосування для регулювання висоти столу, клавіатури і екрану, а також підставка для рук
Пожежна безпека.

Під пожежною безпекою розуміють систему державних і суспільних заходів, спрямованих на охорону від вогню людей і власності. Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки (негорючі речовини й матеріали в холодному стані.

Всі приміщення повинні бути забезпечені первинними засобами пожежегасіння: пожежним водопостачанням (пожежні крани ПК), пожежні щити з набором пожежного інструменту, вуглекислотними або порошковими вогнегасниками. У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефону 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації і приступити до ліквідації пожеж.

Висновок

У дипломному проекті на тему «Розробка комплексних заходів безпеки інформаційних систем студії веб-дизайну» основною метою є аналіз методів та рішень захисту студії веб-дизайну. Безперервність процесів роботи більшості сучасних компаній залежить від надійності сервісів телекомунікаційних компаній. Тому підприємства, що працюють в сфері телекомунікацій, повинні розуміти існуючі загрози та ризикі, складати модель загроз, на основі чого формувати механізми захисту. Застосування технічних засобів охорони – важливий крок до зниження зовнішніх та внутрішніх загроз та підвищення загального рівня безпеки.

Результати роботи такі :

1. Визначено основні поняття інформаційної безпеки студії веб дизану.
2. Проведено аналіз ризиків інформаційних систем.
3. Побудували систему захисту інформацій
4. Визначено принпици КСЗІ в студії веб-дизайну.
5. Провели комплексну систему безпеки інформаційних систем студії веб-дизайну.

В економічному розділі розраховано трудомісткість виконання науково-дослідницької розробки, проведено оцінку тривалості виконання НДР, розраховано собівартість виконання НДР.

У розділі охорони праці й навколишнього середовища проведено аналіз законодавства України про охорону праці, представлено вимоги щодо розміщення і планування приміщень для роботи з комп’ютером, організації та обладнання робочих місць та режим праці та відпочинку при роботі з ПК.

Перелік посилань

1. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: курс лекцій. – К.: КНТ, 2007.-208 с.

2. Бондаренко М.Ф., Черних С.П., Горбенко І.Д., Замула А.А., Ткач А.А.

3. Методические основы концепции и политики безопасности информационных технологий. Радиотехника. 2001. Вып.119.с.5-17.

4. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. НД ТЗІ 1.1-005-07.

5.Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. НД ТЗІ 3.1-001-07.

6.Типове положення про службу захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 1.4-001. [8] Методологічні вказівки щодо розробки ТЗ на створення КСЗІ в АС. НД ТЗІ 3.7-001-99.

7.Бойчик І. М. Економіка підприємства : навчальний посібник для студентів економічних спеціальностей вищих навчальних закладів І-IV рівнів акредитації. 8 Третє видання, випр. і доп. / І. М. Бойчик, П. С. Харів., М. І. Холчан, Ю. В. Піча. – К. : Каравела, 2016. – 328 с.

9. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В Романец., П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

10. Мотузко Ф.Я. Охорона праці - М.: Вища школа, 1989. - 336с.

11. Безпека життєдіяльності. / Под ред. Н.А. Бєлова - М.: Знання, 2000 - 364с.

12.Самгін Е.Б. Освітлення робочих місць. - М.: МІРЕА, 1989. - 186с.

13. Боротьба з шумом на виробництві: Довідник / Є.Я. Юдін, Л.А. Борисов; За заг. ред. Є.Я. Юдіна - М.: Машинобудування, 1985. - 400с., Іл.