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.05.24.000.ДП

Семенюк Олександри 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 методів та засобів захисту інформації комерційного підприємства від несанкціонованого доступу

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на 10 аркушах (слайдах).

Дипломник _____ (Семенюк О. 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 ОНАХТ»

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.

З А В Д А Н Н Я

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти **Семенюк Олександрі Сергіївні**

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): **Розробка методів та засобів захисту інформації комерційного підприємства від несанкціонованого доступу**

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): **Корпоративна мережа підприємства. Безпека підприємства. Технічні засоби обробки інформації. Носії інформації. Технічні засоби захисту інформації. Інформаційна система. Локальна мережа. Захист інформації від витоку. Забезпечення інформаційної безпеки. Доступність информації.**

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.Ризики інформаційніх ресурсів комерційного підприемства.		
4.	Технологічний розділ. Проблеми несанкціонованого доступу до інформації.		
5.	Технологічний розділ. Розробка методів та засобів захисту інформації комерційного підприємства.		
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.05.24.000.ДП	Дипломний проект		
А4			КГ.05.24.000.ДП. ПЗ	Пояснювальна записка	1	
				Презентація	10	

					КГ.05.24. 000.ДП	
Ізм.	Арк.	№ докум.	Підпис	Дата		
Розробив		Семенюк О. С.			Розробка методів та засобів захисту інформації комерційного підприємства від несанкціонованого доступу.	Літ. / Аркуш: Н Д П / 3
Перевірив		Шевцов Ю.С.				ВСП ОТФК ОНТУ
Н. Контр.		Петрашова В.І.				
Затверд.		Скорнякова				

ЗМІСТ

Вступ

Широке застосування комп’ютерних технологій в ком’ютерних системах та мережах, автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп’ютерних системах, від несанкціонованого доступу. Захист інформації в комп’ютерних системах має ряд специфічних особливостей, пов’язаних з тим, що інформація не є жорстко пов’язаною з носієм, може легко і швидко копіюватись та передаватись через канали зв’язку. Відома дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх, так і з боку внутрішніх порушників режиму таємності. Безпека інформації в інформаційній системі чи телекомунікаційній мережі забезпечується здатністю цієї системи зберігати таємність інформації при її введенні, виведенні, передаванні, обробці та зберіганні, а також протистояти її руйнуванню, крадіжкам чи спотворенню. Безпека інформації забезпечується шляхом організації допуску до неї, захисту її від перехвату, спотворення чи введення помилкової інформації. З цією метою застосовуються фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту. Останні посідають центральне місце в системі забезпечення безпеки інформації в інформаційних системах та телекомунікаційних мережах.

1. Ризики інформаційних ресурсів комерційного підприємства.

1.1 Роль інформації в комерційній діяльності

Ефективність комерційної діяльності залежить від наявності у працівників комерційних служб інформації, необхідної для прийняття правильних рішень у ринковій ситуації, яка склалась на певний момент. Під інформацією, в широкому розумінні, вважають дані про кількісний та якісний стан явищ, фактів, предметів, процесів у певний момент часу. Тому дані, що характеризують ситуацію на ринку товарів і послуг, відносяться до комерційної інформації. Комерційна інформація - це інформація по компаніям, фірмам, корпораціям, напрямами їх робіт і продукції, що випускається, фінансовий стан, ділових зв'язках, угодах, керівниках, а також ділові новини в сфері економіки та бізнесу, що надаються інформаційними службами. Комерційна інформація включає дані про :

- попит покупців і фактори, що його визначають;
- місткість ринку;
- товарні пропозиції;
- оптових покупців і продавців товарів;
- платоспроможність покупців товарів;
- конкурентоспроможність і потенційні можливості підприємств;
- прогнозовані обсяги продажу товарів і ціни;
- можливі ризики;
- обсяги продажів товарів і ціни (прогноз).

Інформація про попит покупців використовується під час прийняття комерційних рішень щодо визначення товарного асортименту, обсягів закупки і

продажу товарів, цінової політики, відображення вимоги покупців до рівня якості товарів, мотивів здійснення покупок, ступеня відповідності споживчих властивостей товарів. Вивчення факторів, які впливають на попит, дає можливість комерційним службам отримувати інформацію, необхідну для впливу на формування попиту та приведення пропозиції відповідно до попиту. Аналіз отриманої інформації сприяє найточнішому визначенню структури асортименту, обсягів продажу, рівня якості, цін на товари. При цьому зменшуються ризики закупки чи виробництва товарів, які не користуються попитом, що сприяє прискоренню обігу товарів, збільшенню обсягів продажу. Інформація про місткість ринку дає можливість уникнути дефіциту чи надлишку товарів у певному місті, районі, області. Під час завезення товарів необхідно враховувати попит не тільки місцевого, але й приїжджого населення, підприємств, організацій. Інформація про товарні пропозиції дозволяє встановити співвідношення між попитом і пропозицією, орієнтуватись у ціні ринкової рівноваги. Якщо попит перевищує пропозицію, створюється дефіцит товарів, ціни підвищуються, частина попиту не задовольняється, ринок втрачає стабільність. При перевищенні пропозиції над попитом створюються надлишки товарних запасів, що призводить до затоварення, порушення термінів зберігання товарів, зменшення швидкості товарообігу. Інформація про оптових покупців необхідна для визначення місцезнаходження майбутніх партнерів, їх спеціалізації, можливостей транспортних сполучень, що необхідно для укладення комерційних угод. Платоспроможність оптових покупців товарів сприяє чіткому виконанню договірних зобов’язань, уникненню судових вирішень спорів, зволікання в розрахунках. Від платоспроможності покупців залежить орієнтація роздрібних торговельних підприємств на обсяги товарообігу, рівень якості товарів і цін, додаткових послуг, сервісу тощо. Інформація про конкурентоспроможність і потенційні можливості підприємства - це дані внутрішніх джерел підприємства: статистичних, бухгалтерських звітів, даних оперативного обліку. Щоб зробити висновок про конкурентоспроможність підприємства, необхідний детальніший аналіз діяльності підприємств -

конкурентів. Кожне підприємство повинно передбачити можливі ризики В своїй діяльності. Тому необхідно постійно оцінювати вплив факторів макро- та мікросередовищ на діяльність підприємства. Особливості політичного, економічного, демографічного розвитку, природні, географічні, соціальні особливості повинні враховуватися кожним підприємством як фактори ризику. Аналіз інформації, отриманої під час проведення комплексних маркетингових досліджень ринку, моніторингу не тільки дасть можливість зробити висновки щодо ситуації, яка склалась на ринку, але й прогнозувати стан ринку в майбутньому. Мати достовірну комерційну інформацію означає володіти ситуацією на ринку.

1.2 Комерційна інформація

Комерційна інформація має відповідати таким вимогам:

- достовірність (повинна бути надійною і аргументованою);
- оперативність (своєчасно отримувати цю інформацію);
- систематичність (інформація повинна надходити безперервно, систематично і постійно оновлюватися);
- комплектність (має відображати діяльність суб’єкта господарювання).

Інформація тісно пов’язана з ризиком комерційної діяльності. Суть і зміст комерційного ризику. Діяльність підприємства завжди пов'язана з невизначеністю. Наявність невизначеності в діяльності комерційних суб'єктів, або іншими словами, ймовірного характеру в проходженні подій, пов'язаних з функціонуванням всіх елементів ринку, обумовлює виникнення ризиків, без врахування яких неможливий ефективний розвиток підприємств. Економічний ризик - об'єктивно-суб'єктивна категорія, яка пов'язана з подоланням невизначеності та конфліктності у ситуації неминучого вибору і відображає міру

(ступінь) досягнення сподіваного результату, невдачі та відхилення від цілей з урахуванням впливу контрольованих та неконтрольованих чинників за наявності прямих та зворотних зв'язків. Особливо обтяжена ризиком комерційна діяльність. Комерційний ризик - це ризик, що виникає внаслідок будь-яких видів діяльності, пов'язаних з виробництвом продукції, товарів, послуг, їх реалізацією, товарно-грошовими і фінансовими операціями, комерцією, здійсненням соціально-економічних і науково-технічних проектів. У цих видах діяльності мають справу з використанням і оборотом матеріальних, трудових, фінансових, інформаційних (інтелектуальних) ресурсів, тобто ризик, пов'язаний з повною чи частковою загрозою втрати цих ресурсів. Визначають ризик як загрозу зазнати збитків у вигляді додаткових затрат, непередбачених у прогнозах, проектах, програмах, або ж одержати доходи, менші за очікувані. Причому, якщо затрати необхідні у будь-якому випадку, то збитки є наслідком невизначеності. Об'єктом ризику називають економічну систему, ефективність та умови функціонування якої наперед точно не відомі. Під суб'єктом ризику розрізняють особу (індивід або колектив), яка зацікавлена в наслідках керування об'єктом ризику і компетентна приймати рішення щодо об'єкта ризику. Джерело ризику - це чинники (явища, процеси), які спричиняють невизначеність результатів (конфліктність). Основне призначення комерційної інформації – планування комерційної діяльності її аналіз, контроль за її результатами.

1.1 Аналіз ризиків безпеки інформаційної системи підприємства

Функціонування підприємства пов’язане з інноваційними процесами, розробкою та виробництвом нової продукції, робіт, послуг. Інноваційна діяльність, прагнення до конкурентної переваги змушує компанію впроваджувати новітні досягнення науки, нову продукцію і технологію, нову систему управління працею та виробництвом з метою утримання передових ринкових позицій, що поєднується з численними ризиками, вплив яких на результати господарювання компанії може бути доволі значний. Розвиток

інформаційної інфраструктури підприємства тягне за собою неконтрольоване збільшення кількості вразливостей інформаційних ресурсів та інформаційних загроз, основними типами джерел яких є природні, техногенні і людські. Є методи, що дозволяють провести аналіз рівня ризиків інформаційної безпеки і оцінити оптимальні витрати підприємства на захист інформації. Аналіз ризиків передбачає процедуру виявлення чинників ризиків, оцінку їх значимості і методи зниження ризиків або зменшення пов'язаних із цим несприятливих наслідків. Актуальні задачі аналізу і оцінки ризиків інформаційної безпеки дозволяють визначити необхідний рівень захисту інформації, а також розробити рекомендації щодо вдосконалення системи захисту і мінімізації ризиків. Розв'язання проблеми забезпечення кібербезпеки інформаційних ресурсів вимагає підготовки та прийняття організаційних і технічних заходів, розробка яких базується на запропонованих підходах.

В умовах прискореної динаміки розвитку інформатизації суспільства спостерігається щорічна тенденція зростання кіберзагроз інформаційним ресурсам, тому їх захист є однією з важливих проблем. Розв'язання такої задачі вимагає підготовки і прийняття організаційних і технічних заходів щодо забезпечення кібербезпеки інформаційних ресурсів підприємств. Поняття ризику, як відомо, є наслідком тісної взаємодії таких понять, як актив, вразливість, загроза і збиток. Активи – це ключові компоненти інфраструктури і важлива інформація, яка опрацьовується в інформаційній системі. До основних активів відносять бізнес-процеси – сукупність видів діяльності, в результаті якої створюється продукт або послуга, що становить інтерес для споживача. Основним активом виступає також інформація – відомості, які є предметом власності, що підлягають захисту від порушення конфіденційності, цілісності та доступності відповідно до вимог правових документів і вимог власника інформації, незалежно від форми подання, зокрема, інформаційні ресурси (бази і файли даних, системна документація, науково-дослідна інформація та документація, контракти і угоди тощо). До допоміжних активів належить, насамперед, апаратно-програмний комплекс - сукупність технічних і програмних

засобів, призначених для виконання взаємозалежних експлуатаційних функцій з обробки інформації обмеженого поширення, що включає в себе активну апаратуру обробки даних, стаціонарну апаратуру, периферійні пристрої, операційні системи та прикладне програмне забезпечення. До цієї ж категорії входять носії даних; сукупність телекомунікаційних пристроїв, що використовуються для з'єднання декількох фізично віддалених сегментів інформаційної системи; співробітники компанії, їх кваліфікація і досвід, а також нематеріальні ресурси (репутація і імідж компанії). Вразливість – слабке місце в засобах захисту, спричинене помилками чи недосконалістю процедур, проектів, реалізації, яке загроза може подолати. Іншими словами, вразливості – це будь-які чинники, що роблять можливою успішну реалізацію загроз. Практика свідчить, що вразливості є основною причиною виникнення атак. Загрозою вважають потенційну можливість причинити збиток якимось наперед відомим способом. Загрози інформаційній безпеці можуть бути здійснені шляхом використання вразливостей системи. Слабкості захисту можуть використовуватися однією або декількома загрозами, що є причиною небажаних інцидентів, які можуть призвести до нестабільного функціонування компонентів інформаційної системи. Наявність слабких місць в захисті інформаційної системи може бути обумовлена різними чинниками, починаючи з простої недбалості співробітників і закінчуючи навмисними діями зловмисників. Збиток складають витрати на відновлення системи після можливого порушення інформаційної безпеки. Наявність ризику – це ймовірність того, що відбудуться певні небажані події, які можуть негативно вплинути на досягнення цілей конкретного бізнес-процесу. Зокрема, функціонування підприємства в пов'язане з інноваційними процесами, розробкою та виробництвом нової продукції, робіт, послуг. Інноваційна діяльність, прагнення до конкурентної переваги змушує компанію впроваджувати новітні досягнення науки, нову продукцію і технологію, нову систему управління працею та виробництвом з метою утримання передових ринкових позицій, що поєднується з численними ризиками, вплив яких на результати господарювання компанії доволі значний. У зв'язку із цим своєчасна,

оперативна і коректна оцінка ризиків зниження або повної втрати інформаційної безпеки сьогодні є актуальною проблемою в діяльності будь-якої організації. Інформаційна безпека, визначаючи рівень захищеності бізнес-середовища, стає важливим аспектом загальної економічної безпеки в діяльності сучасної компанії. Захист інформації – особливий вид діяльності щодо запобігання витоку інформації, несанкціонованих змін її потоків та інших чинників, які негативно впливають на стабільну роботу підприємства і пов'язаних з ним економічних партнерів (клієнтів, постачальників обладнання, інвесторів та ін.). Аналіз останніх досліджень і публікацій. Розвиток інформаційної інфраструктури підприємства тягне за собою неконтрольоване збільшення кількості інформаційних загроз і вразливостей інформаційних ресурсів. Сучасні дослідження відзначають такі типи джерел загроз, що впливають на інформаційну безпеку: природні; техногенні; людські навмисні і людські ненавмисні. Для підприємств інноваційного типу, характерні наступні види ризиків діяльності: організаційні (низька кваліфікація розробників проекту, затримка виконання етапів його реалізації); науково-технічні (зношеність технологічного обладнання, відсутність резервів потужностей або типових проектних рішень); фінансово-економічні (маркетинговий, ризик фінансування проекту, інфляційний, процентний, податковий і операційний ризики). У сучасних умовах перед кожним підприємством, яке дбає про безпеку своїх інформаційних ресурсів, постає питання про організацію системи захисту інформації, що дозволила б гарантувати безпеку функціонування телекомунікаційного обладнання і циркулюючої інформації в інформаційній системі підприємства. Ефективність захисту інформації залежить від підходу до її організації та правильного вибору методів розрахунку ризиків інформаційної безпеки. Існує чимало методик оцінки та опрацювання ризиків, які можуть застосовуватися до будь-якої інформаційної системи, незалежно від рівня конфіденційності наявної інформації. Однак, зазвичай, для якісної побудови системи захисту інформації з використанням таких методик потрібен значний обсяг інформації про потенційні атаки, а також про спроби їх реалізації, який

підлягає програмному аналізу з метою виявлення найбільш актуальних загроз інформаційній безпеці. Аналіз ризиків передбачає процедуру виявлення чинників ризиків, оцінку їх значимості і методи зниження ризиків або зменшення пов'язаних із цим несприятливих наслідків. Актуальні задачі аналізу і оцінки ризиків інформаційної безпеки дозволяють визначити необхідний рівень захисту інформації, а також розробити рекомендації щодо удосконалення системи захисту і мінімізації ризиків. Аналіз ризиків поділяють на два види: якісний і кількісний. Якісний аналіз дозволяє визначити (ідентифікувати) чинники, області та види ризиків. Кількісний аналіз ризиків дає можливість чисельно визначити розміри окремих ризиків і загальний розмір ризику в цілому. Підсумкові результати якісного аналізу ризиків, у свою чергу, можуть стати вхідною інформацією для проведення кількісного аналізу. Однак для здійснення кількісного аналізу ризиків потрібна надійна вхідна інформація (збір статистичної інформації ускладнений жорсткою конкуренцією в бізнесовому середовищі) і чітко визначена шкала оцінки параметрів. Процес розрахунку ризиків інформаційної безпеки актуальний на всіх етапах роботи системи захисту інформації та є цікавим для власника інформації, насамперед, з точки зору втрат в економічній сфері. Вибір методу оцінки ризиків інформаційної безпеки в більшості випадків ґрунтується на таких чинниках: часові, фінансові, інформаційні ресурси; ступінь невизначеності оцінки ризиків інформаційної безпеки; наявність або відсутність можливості отримання кількісних оцінок вхідних даних, де вхідними даними можуть бути висновки, рішення, переліки, а також рекомендації, залежно від методу та етапу оцінки ризиків інформаційної безпеки. Разом із тим у процесі оцінки ризиків повинні бути встановлені критерії прийнятності ризику та критерії для оцінки ризиків інформаційної безпеки, а також повинні бути дані гарантії того, що аналіз ризиків дасть надійні і несуперечливі масиви актуальних для даної системи ризиків. Необхідно провести ідентифікацію ризиків інформаційної безпеки, спрямованих на такі властивості інформаційних ресурсів, як конфіденційність, цілісність і доступність. Потрібно виконати ідентифікацію власника ризику, де під

власником розуміється фізична, юридична особа або підрозділ, що відповідає за управління ризиком і має необхідні для цього повноваження, в даному випадку, мова може йти про керівників, фахівців з інформаційної захисту, відділів з інформаційної безпеки тощо. Аналіз і оцінка ризиків в задачі управління інформаційною безпекою на сьогодні – одне із складних і актуальних завдань. Складність полягає в тому, що відсутні загальноприйняті підходи і методики для оцінки ризиків. Чинники ризику (загроза, вразливість, збиток) аналізуються за допомогою евристичних методів, які містять суб'єктивну складову частину. У процесі аналізу ризиків інформаційної безпеки здійснюється оцінка потенційних втрат у випадку реалізації ризику, оцінюється ймовірність реалізації ризиків і визначається величина ризиків. У ході оцінки ризиків інформаційної безпеки має бути виконано порівняння ризиків із встановленими критеріями, а також визначено вектор пріоритетних напрямків з їх опрацювання.

Таблиця 2.

Класифікація небезпек і загроз економічній безпеці підприємства

Ознака	Класифікація
По можливості прогнозування:	*прогнозовані* – що виникають при певних обставинах, виявлені на підставі минулого досвіду, узагальнені галузевою наукою та прикріплені в законах, стандартах, технічних умовах та інших нормативних документах; *непередбачені* – форс-мажорні обставини, технологічні досягнення й відкриття та інщі, неминучі по суті.
по джерелу походження:	*об'єктивні* – виникають без участі та волі суб'єктів системи (стан ринкової кон'юнктури, конкурентний перерозподіл ринку і та ін.); *суб'єктивні* – навмисні або ненавмисні дії людей, органів влади або державних організацій; конкурентна боротьба,

	злочинність та інше, що впливають на економічні відносини підприємства на ринку.
по можливості запобігання:	*форс-мажорні* – відрізняються непереборністю впливу (природні катаклізми, техногенні катастрофи, війни, епідемії, які змушують вирішувати й діяти всупереч наміру) і представляють особливу складність запобігання бюджетними коштами; *передбачувані* – можуть бути передбачені на стадії планування бізнесу, процесів і технологій для мінімізації або повного запобігання можливого збитку у випадку реалізації фактору ризику.
по ймовірності настання:	*Явні, очевидні* -обумовлені ринковими (економічними і юридичними) законами; *латентні* – неявні, тимчасово сховані, що важко виявляються. Їхній прояв або невияв може бути зумовлений економічною кон'юнктурою, наслідком макроекономічних явищ, а також конкурентною боротьбою й способами її ведення. Раптовість їх прояву може мати суб'єктивний характер і важко прогнозована навіть при відомій імовірності настання.
по природі їх виникнення:	*економічн*і - кон'юнктурні (ринкові) зміни; *політичні* - зміна влади, введення ембарго; *правові* – законодавче регулювання діяльності, ліцензування; *техногенні* – аварії та катастрофи; *екологічні* – виснаження ресурсів, кліматичні зміни; *конкурентні* – «чорний PR», недобросовісна

	конкуренція; *контрагентські* – невиконання зобов'язань, шахрайство.
по значимості або істотності збитку:	*несуттєві* – що не впливають на ринковий стан компаній; *істотні* – втрата значної частини матеріальних і фінансових ресурсів; *значні* – втрата конкурентних переваг, можливе банкрутство; *катастрофічне* – неможливе продовження господарської діяльності,
по ступеню ймовірності:	*неймовірні* – за вкрай низької ймовірності збігу обставин виникнення погрози; *малоймовірні* – не вимагають планування превентивних заходів як *різновид* форс-мажорних обставин; *імовірні* – слабко прогнозовані, вимагають планування залежно від значимості збитку; *досить імовірні* – прогнозовані, плановані й забезпечені бюджетом; *неминучі* – легко прогнозовані, обумовлені природою виникнення, плановані й забезпечені бюджетом.
за ознакою їх здійснення в часі:	*безпосередня* – з повною ймовірністю здійснення; *близька* (до 1 року) – прогнозована й планована; *далека* (понад 1 рік) – не передбачається поточним бюджетом.
за ознакою їх здійснення в просторі:	*на території підприємства;* *на території, що прилягає до підприємства;* *на території регіону;* *на території країни;* *на закордонній території.*

за способами здійснення:	*промислове шпигунство;* *розкрадання;* *вербування і підкуп персоналу;* *психологічний вплив на персонал;* *технологічний доступ та інші.*
за сферою виникнення:	*внутрішні фактори* - пов'язані з господарською діяльність підприємства і його персоналу. Обумовлені бізнес – процесами, що й зумовлюють вплив на результати господарської діяльності підприємством, дотримання технологій, організація праці й соціальної сфери персоналу й багато інших; *зовнішні* – виникають за межами підприємства, пов'язані з кон'юнктурою ринку й середовищем функціонування підприємства, їх зміна може привести до виникнення збитків: соціально-економічних, політичних, юридичних, технологічних криміналістичних тощо.

При класифікації поєднуємо – матеріальні цінності та фінансові ресурси. Схематично, це виглядає наступним чином:

Рис. 1. Класифікація загроз економічної безпеці, в залежності від об'єкту впливу

Дана класифікація, дозволяє вже працівникам підрозділів (до функціональних обов'язків яких входить захист економічних інтересів) проводити роботи спрямовані на своєчасне виявлення, локалізацію, нейтралізацію та по можливості усунення загроз, які впливають на економічну безпеку.

2.Проблеми несанкціонованого доступу до інформації

Несанкціонований доступ до інформації — доступ до інформації з порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Причини несанкціонованого доступу до інформації

- помилки конфігурації (прав доступу, брандмауерів, обмежень на масовість запитів до баз даних)
- слабка захищеність засобів авторизації (розкрадання паролів, смарт-карт; фізичний доступ до устаткування, що погано охороняється; доступ до незаблокованих робочих місць співробітників під час відсутності співробітників)
- помилки в програмному забезпеченні
- зловживання службовими повноваженнями (викрадення резервних копій, копіювання інформації на зовнішні носії при праві доступу до інформації)
- прослуховування каналів зв'язку при використанні незахищених з'єднань всередині ЛОМ
- використання клавіатурних шпигунів, вірусів і троянів на комп'ютерах співробітників.

2.1 Кроки для отримання несанкціонованого доступу

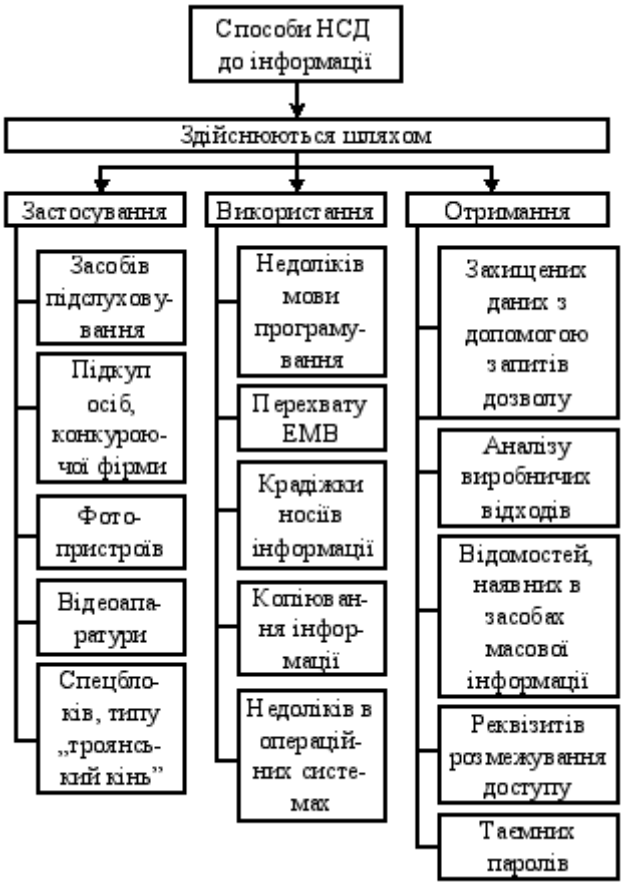
- Збір інформації щодо IT профілю жертви, так званого цифрового сліду (англ. *footprint*)
- Аналіз інформації, насамперед відкритих TCP, UDP портів та існуючих способів отримання доступу до комп'ютерної мережі жертви
- Отримання логінів і паролів користувачів із застосуванням:

-Методом соціальної інженерії, як правило хакер видає себе за співробітника IT відділу компанії, якому необхідна інформація, щодо облікових даних користувача для вирішення якихось надуманих проблем

-Отримання доступу до паперового сміття жертви

-Спеціальних програм для злому паролів. Ці програми використовують списки слів, фраз, або інших комбінацій букв, цифр і символів, які користувачі комп'ютерів часто використовують як паролі

- Якщо вдається отримати доступ до комп'ютерної мережі жертви, хакер намагається набути адміністраторських привілеїв. Для цього ведеться пошук на файлових системах та використовуються трояни
- Після отримання адміністраторських привілеїв хакер проводить детальний аналіз комп'ютерної системи жертви, отримуються доступ до баз даних, веб серверів та інших комп'ютерних ресурсів
- Організація так званого бекдор — *чорного входу*. Хакер створює нестандартні методи отримання доступу до мережі жертви для запобігання свого виявлення і блокування IT спеціалістами компанії.



Мал.1. Способи НСД до інформації

Починаючи з 90-х років минулого століття, паралельно із вдосконаленням ринкових відносин змінювалися форми впливу правопорушників на об’єкти зі стабільним фінансовим становищем:

• початковий етап — психологічні атаки (шантаж, погрози) і фізичні розправами;

• другий етап — недобросовісна конкуренція, неділове партнерство, поява фіктивних фірм, агентів у штаті конкуруючих підприємств і т. д.;

• третій етап — несанкціонований доступ до інформації будь-якими способами, в тому числі й програмними, за рахунок перехоплення паразитного електромагнітного випромінення і наведення (ПЕМВН) в ефірі або за рахунок наведення побічних випромінень на провід електроживлення.

Провода електроживлення і заземлення створюють рамкову антену, тому рівень випромінення комп’ютера збільшується. Ситуація з забезпеченням безпеки стає ще більш уразливою у зв’язку із всезагальною комп’ютеризацією підприємництва.

Корисно нагадати такі аксіоми:

• за забезпечення збереження інформації треба платити, а за відсутність такої — розплачуватися;

• доки не буде вироблено заходів для безпосереднього захисту засобів телекомунікації, в тому числі й засобів обчислювальної техніки (ЗОТ), будь-які інші спроби захистити інформацію марні.

2.2 Канали відтоку інформації

Виникла необхідність розробити технологію захисту інформації, за якої змінні параметри засобів обчислювальної техніки суттєво не впливали б на процес виробництва засобів захисту і виробів у цілому. Найвідоміші сьогодні перехоплення - це випромінення моніторів. Монітор є “найголоснішим” випромінюючим елементом, оскільки для нормальної роботи електронно-променевої трубки необхідні високі рівні сигналів. Для дешифрування перехоплених сигналів монітора не потрібно складного опрацювання. Зображення на екрані монітора і, відповідно, випромінювані ним сигнали багаторазово повторюються. У професійній апаратурі ця обставина використовується для накопичення сигналів і, відповідно, ефективнішої діяльності розвідки. Професійна апаратура для перехоплення випромінення монітора і відображення інформації коштує десятки тисяч доларів. Якщо розвідувальна апаратура встановлена на невеликій відстані, наприклад, у сусідній квартирі, то для перехоплення випромінення монітора може використовуватися саморобна апаратура, найдорожчим елементом якої є монітор комп’ютера, або навіть дещо доопрацьований побутовий телевізор. Перехоплення інформації за рахунок випромінення принтерів, клавіатури обійдеться ще дешевше. Інформація у цих пристроях перехоплюється послідовним кодом, усі параметри якого стандартизовані й широко відомі.

Адміністратори локальної комп’ютерної мережі застосовують усі можливі засоби для розмежування доступу, входять у мережу лише з визначеної станції, коли нікого немає. Однак їм необхідно пам’ятати про радіовипромінення, а непоганий малогабаритний професійний розвідувальний приймач нині коштує лише кілька сотень доларів. Інформація, що передається в ефір за рахунок випромінення принтерів і клавіатури, - це фактично метод радіорозвідки з використанням прихованого випромінення. Комп’ютер може випромінювати в ефір не лише ту інформацію, що опрацьовує. Якщо при його збиранні не було вжито спеціальних заходів, то він може слугувати також і джерелом відтоку мовної інформації. Це так званий “мікрофонний ефект”, він може здійснюватися навіть через корпус комп’ютера. Під впливом акустичних коливань у корпусі змінюються розміри щілин і інших елементів, через які здійснюється випромінення. Відповідно, випромінення стає модульованим, і все, що ви говорите біля комп’ютера, можна прослухати за допомогою розвідувального приймача. Якщо ж до комп’ютера підключені звукові колонки, то шпигун взагалі може заощадити на встановленні у приміщені, що прослуховується, “жучків”. Таким чином, щоб уникнути відтоку інформації через канали паразитного випромінення, необхідно захищатися.

2.3 Засоби боротьби з проникненням

Методи проникнення у комп’ютерну мережу з метою наступного викрадення інформації різноманітні, найдієвий - це встановлення в системі програми-закладки. Програма-закладка, залежно від поставленої мети, може, наприклад, перехоплювати паролі користувачів або за визначеним критерієм знаходити необхідну інформацію на жорстких дисках. Усі системні адміністратори вживають відповідних заходів з попередження спроб відправити електронною поштою зібрану правопорушником інформацію на завчасно обумовлену адресу. Це змусить порушників вигадувати нові методи

проникнення до комп'ютерної мережі. Розвідувальну діяльність правопорушника найбільше ускладнюють два моменти:

• встановити програму-закладку ("троянського коня");

• передати перехоплену інформацію.

На заваді розвідувальної діяльності стоять великі обсяги програми-закладки та даних, що передаються за її допомогою. Скільки існує людство, стільки існує й проблема обміну інформацією. З однієї сторони, люди прагнуть спілкуватися і обмінюватися інформацією, а з іншої, намагаються приховати від сторонніх як зміст, так і факт її передачі. Тому людство постійно удосконалює засоби перехоплення і приховування. Для приховування інформації застосовують методи криптографії і стеганографії.

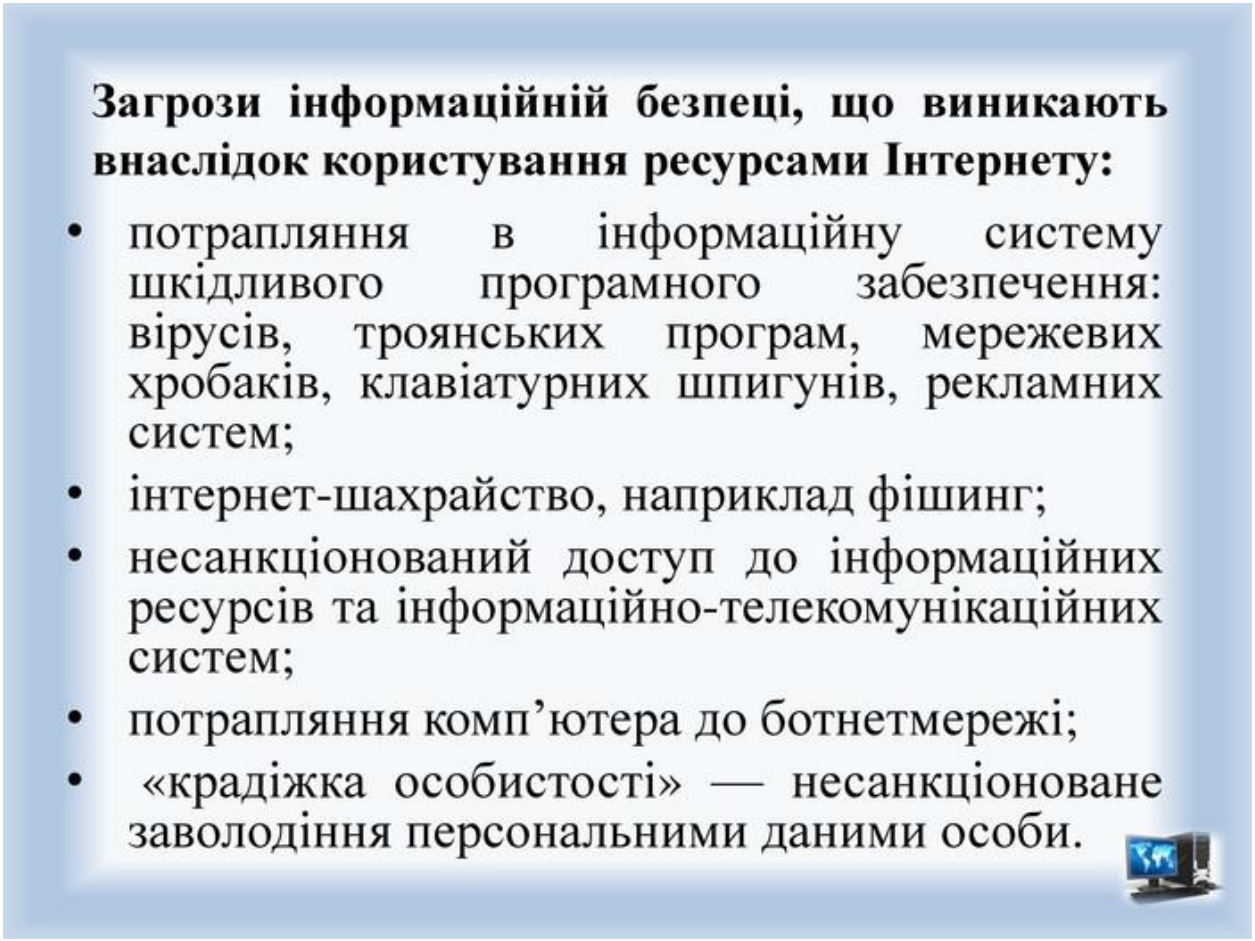
Криптографія — це система зміни інформації, щоб вона була зрозумілою лише для посвячених.

Стеганографія — це система зміни інформації з метою приховування самого факту існування таємного повідомлення. Слово "стеганографія" походить від слів "steganos" — таємниця і "graphy" — запис і буквально означає "таємний запис".

Застосування криптографії дозволяє сторонньому спостерігачеві легко встановити факт передачі таємного повідомлення, а стеганографії — приховувати це, більше того, для підвищення рівня захисту таємна інформація може додатково шифруватися. Методи стеганографії передбачають, що сам факт будь-якого обміну інформацією не приховується, хоча повідомлення обов'язково переглядає цензор. Тому під приховуванням факту існування таємного повідомлення розуміється не лише (можливо, навіть не стільки) те, що цензор не може виявити у повідомлені, яке переглядається, іншого, прихованого повідомлення, а й те, що переказуване повідомлення не повинно викликати у цензора підозри.

2.4 Аналіз способів несанкціонованого доступу до інформації в комп'ютерних системах

Розмежування доступу до елементів полягає в тому, щоб кожному зареєстрованому користувачу надати можливості безперешкодного доступу до інформації в межах його повноважень і виключити можливості перевищення своїх повноважень. Розмежування доступу користувачів систем може здійснюватися за декількома параметрами: виглядом, характером, призначенням, ступенем важливості і секретності інформації. При проектуванні систем діагностичного центру потрібно розробити і реалізувати функціональність щодо контролю доступу до апаратури та інформації, як в рамках інформаційної системи в цілому, так і до окремих інформаційних частин.



Мал.2. Загрози інформаційній безпеці

Першим етапом розмежування доступу стає автентифікація, яка являє собою процедуру перевірки дійсності ідентифікаторів. Спочатку здійснюється ідентифікація – перевіряється приналежність пред'явленого ідентифікатора, безлічі зареєстрованих у системі. У випадку коректності ідентифікатора, виконується автентифікації по перевірці паролю, щоб переконатися, що користувач є саме тим, за кого себе видає. Допуск претендента в систему дозволяється тільки у випадку успішного завершення процедури автентифікації. Під загрозою безпеки інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів програмної системи, а також програмних і апаратних засобів. Усі можливі способи несанкціонованого доступу до інформації в комп'ютерних системах, можна класифікувати за наступними ознаками:

1) За принципом несанкціонованого доступу:

- фізичне подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; розкрадання документів і носіїв інформації; візуальне перехоплення інформації, виведеної на екрани моніторів і принтери, а також підслуховування; перехоплення електромагнітних випромінювань.
- логічне подолання системи захисту ресурсів активної комп'ютерної мережі.

2) По положенню джерела несанкціонованого доступу:

- внутрішнє розташування джерела. Атака проводиться безпосередньо з будь-якої точки локальної мережі; ініціатором атаки найчастіше виступає санкціонований користувач.
- зовнішнє розташування джерела взлому. Зазвичай несанкціоновані дії в закриту мережу (захищену) відбуваються із відкритої; атака на окремі мережі, орієнтовані на обробку конфіденційної інформації зовсім різного рівня чи секретності різних категорій.

3) По режиму виконання несанкціонованого доступу:

- атаки, причиною яких є людина;

- атаки, причиною яких є спеціально розроблена програма без особистої участі людини. При такому виді несанкціонованого доступу використовуються спеціально розроблені програми, в основу функціонування яких покладена вірусна технологія.

4) За типом використаних уразливих місць систем:

- атаки, основані на недоліках встановленої політики безпеки. При такому виді несанкціонованого доступу політика безпеки не відображує реальні аспекти обробки інформації.

- атаки, основані на помилках управління та адміністрування комп'ютерною мережею. При такому виді несанкціонованого доступу мається на увазі некоректна організаційна реалізація чи недостатня адміністративна підтримка прийнятої в комп'ютерній мережі політики безпеки (через неуважність адміністратора певний каталог доступний усім користувачам).

- непродумані алгоритми захисту, реалізовані у засобах інформаційно-комп'ютерної безпеки;

- неякісна реалізація засобів системи захисту інформації.

5) По шляху несанкціонованого доступу:

- атаки, орієнтовані на використання прямого стандартного шляху доступу до комп'ютерних ресурсів. При такому виді несанкціонованого доступу мається на увазі недоліки політики безпеки; недоліки процесу адміністративного управління комп'ютерною мережею.

- атаки, орієнтовані на використання схованого нестандартного шляху доступу до комп'ютерних ресурсів. При такому виді доступ здійснюються шляхом використання недокументованих особливостей системи інформаційно-комп'ютерної безпеки.

6) По поточному місцю розташуванню кінцевого об'єкта атаки:

- атаки на інформацію, яка зберігається в основній пам'яті комп'ютера

- атаки на інформацію, що зберігається на зовнішніх запам'ятовуючих пристроях;

- атаки на інформацію, яка передається по лініях зв'язку.

7) По безпосередньому об'єкту атаки:

- атаки на політику безпеки і процес адміністративного управління;
- атаки на саму систему захисту та її компоненти;
- атаки на змінні елементи системи безпеки;
- напади на функціональні особливості комп'ютерної системи;
- напади на протоколи взаємодії між користувачами чи компонентами.

Щоб пройти автентифікації можуть використовуватися різні принципи, такі як знання користувачем секретного паролю; пред’явлення користувачем певних статичних характеристик (наприклад, біометрія); встановлення дійсності користувача третьою стороною. Часто для надійності використовуються різні комбінації цих принципів.

3. Розробка методів та засобів захисту інформації комерційного підприємства

Щоб в повній мірі задовільнити потреби сучасного суспільства, виникла необхідність інформаційного забезпечення всіх сфер діяльності людини і, зокрема, надійного захисту інформації. Особливої гостроти дана проблема набуває у зв'язку з масовою комп'ютеризацією, об'єднанням комп'ютерів у комп'ютерні мережі та використання Internet.

Інформація – абстрактне поняття, що має різні значення залежно від контексту. Походить від латинського слова «informatio», яке має декілька значень:

– роз'яснення;

– виклад фактів, подій;

– тлумачення;

– представлення, поняття;

– ознайомлення, просвіта.

У кібернетиці інформація трактується зазвичай як міра усунення невизначеності знання у одержувача. Іншими словами, інформацією є не будь-яке повідомлення, а лише таке, яке містить невідомі раніше його одержувачеві факти. У законі України «Про інформацію» наведене таке тлумачення поняття інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Отже можна визначити інформацію як нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисні. Іншими словами, інформація – це нові знання, які отримує суб'єкт у результаті сприйняття і опрацювання певних відомостей. Інформацію розрізняють і за галузями знань: технічна, економічна, біологічна та інші. Найважливішими, з практичної точки зору, властивостями інформації є:

Цінність інформації – визначається забезпеченням можливості досягнення мети, поставленої перед отримувачем інформації.

Достовірність – відповідність отриманої інформації об'єктивній реальності навколишнього світу.

Актуальність – це міра відповідності цінності та достовірності інформації поточному часу (певному часовому періоду). Часові властивості визначають здатність даних передавати динаміку зміни ситуації (динамічність).

Оперативність – властивість даних, яка полягає в тому, що час їхнього збору та переробки відповідає динаміці зміни ситуації;

Ідентичність – властивість даних відповідати стану об'єкту. Для людини інформація поділяється на види залежно від типу рецепторів, що сприймають її.

Візуальна – сприймається органами зору.

Аудіальна – сприймається органами слуху. Тактильна – сприймається тактильними рецепторами.

Нюхова – сприймається нюховими рецепторами.

Смакова – сприймається смаковими рецепторами За формою подання інформація поділяється на такі види:

Текстова – що передається у вигляді символів, призначених позначати лексеми мови;

Числова – у вигляді цифр і знаків, що позначають математичні дії;

Графічна – у вигляді зображень, подій, предметів, графіків;

Звукова – усна або у вигляді запису передачі лексем мови аудіальним шляхом.

За призначенням інформацію також можна поділити на такі види:

Масова – містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму.

Спеціальна – містить специфічний набір понять, при використанні відбувається передача відомостей, які можуть бути не зрозумілі основній масі соціуму, але необхідні і зрозумілі в рамках вузької соціальної групи, де використовується дана інформація

Особиста – набір відомостей про яку-небудь особистість, що визначає соціальний стан і типи соціальних взаємодій всередині популяції.

У законодавстві Україна виділяють інформацію з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Інформація з обмеженим доступом – інформація, право доступу до якої обмежене встановленими правовими нормами та (або) правилами.

Інформація таємна (secret information) – інформація з обмеженим доступом, що містить відомості, які становлять державну та іншу передбачену законом таємницю і розголошення яких завдає шкоди особі, суспільству та державі.

Інформація конфіденційна – інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави, і порядок доступу до якої встановлюється ними.

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Російський автор В.Н. Ясенєв дає більш цікаве тлумачення поняття «конфіденційність», а саме конфіденційність комп'ютерної інформації, з його точки зору це властивість інформації бути відомою лише допущеним та пройшовшим перевірку суб'єктам системи (користувачам, програмам, процесам та ін.). Отже можна зробити висновки, що існує така інформація, яка потребує захисту.

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. У тому ж законі про інформацію поняття захист інформації визначається як, сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Захист – засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні, в тому числі програмні, заходи запобігання несанкціонованого доступу до апаратури, програм і даних.

Метод захисту (protection method) – система принципів і прийомів, спрямованих на реалізацію функції захисту. Метод захисту може бути реалізований програмним, програмно-апаратним або апаратним способом .

Захист інформації ведеться з метою підтримки таких властивостей інформації як:

- цілісність
- неможливість модифікації інформації неавторизованим користувачем.

Цілісність інформації важливий аспект інформаційної безпеки, що забезпечує запобігання несанкціонованих змін та руйнування інформації .

Цілісність, це стан даних або комп'ютерної системи, в якій дані та програми використовуються встановленим чином, що забезпечує: стійку роботу системи; автоматичне відновлення у випадку виявлення системою потенційної помилки; автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу;

- конфіденційність – інформація не може бути отримана неавторизованим користувачем. Треба захисти інформацію від несанкціонованого ознайомлення з нею.
- доступність – полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

У літературних джерелах розглядається ряд заходів для захисту інформаційної системи. Зокрема автори виділяють: - законодавчі (закони, нормативні акти, стандарти та ін.);

- адміністративні (дії загального характеру організації, що робляться керівництвом);

- процедурні (конкретні заходи безпеки, що мають справу з людьми);
- програмно-технічні (для ідентифікації і перевірки автентичності користувачів; управління доступом; протоколювання і аудиту; криптографії; екранування та ін.). Апаратно-програмні засоби захисту – засоби у яких програмні (мікропрограмні) та апаратні частини повністю взаємопов’язані та нероздільні. Апаратні засоби захисту – це електронні, електромеханічні та інші пристрої, безпосередньо вбудовані у блоки автоматизованої інформаційної системи або оформлені у вигляді самостійних пристроїв які сполучаються з цими блоками. Вони призначені для внутрішнього захисту структурних елементів засобів та систем обчислюваної техніки: терміналів, процесорів, периферійного устаткування, ліній зв’язку та інше.

Завданням забезпечення безпеки (захисту) інформації є: - захист інформації в каналах зв’язку та базах даних криптографічними методами; - підтвердження справжності об’єктів даних та користувачів (аутентифікація сторін, що встановлюють зв'язок); - виявлення порушень цілісності об’єктів даних; - забезпечення захисту технічних засобів та приміщень, в яких ведеться обробка конфіденційної інформації, від витоку через побічні канали і від можливо вбудованих в них електронних пристроїв знімання інформації; - забезпечення захисту програмних продуктів та засобів обчислювальної техніки від внесення в них програмних вірусів та закладок; - захист від несанкціонованих дій через канал зв’язку від осіб, що не допущені до засобів шифрування, але що переслідують цілі компрометації таємної інформації і дезорганізації роботи абонентських пунктів; - організаційно-технічні заходи, спрямовані на забезпечення збереження інформації з обмеженим доступом; - виконання вимог з кібербезпеки в інформаційних мережах

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми -

комп'ютерні злочини стали характерною ознакою сьогодення. Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби. Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є наступні: - швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях; - широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів; - постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць. Сьогодні ніхто не може назвати точну цифру загальних збитків від комп’ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників КС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей. У сфері захисту інформації та комп’ютерної безпеки в цілому найбільш актуальними є три групи проблем: - порушення грифу обмеження доступу; - порушення цілісності інформації; - порушення дієздатності інформаційно-обчислювальних систем. Захист інформації перетворюється у найважливішу проблему державної безпеки, коли мова йде про державну, дипломатичну, військову, промислову, медичну, фінансову та іншу таємну інформацію. Величезні масиви такої інформації зберігаються в електронних архівах, оброблюються в інформаційних системах та передаються через телекомунікаційні мережі. Основні властивості цієї інформації – конфіденційність та цілісність, повинні підтримуватись законодавчо, юридично, а також організаційними, технічними та програмними методами. Згідно із Законом України «Про захист інформації в автоматизованих системах» захист

інформації - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій». Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно- технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту. Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними причинами порушення безпеки інформації можна назвати такі: - несанкціонований доступ - доступ до інформації, що здійснюється з порушенням установлених в КС правил розмежування доступу; - витік інформації - результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї; - втрата інформації - дія, внаслідок якої інформація в КС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі; - підробка інформації - навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в КС; - блокування інформації — дії, наслідком яких є припинення доступу до інформації; - порушення роботи КС - дії або обставини, які призводять до спотворення процесу обробки інформації. Причини настання зазначених випадків такі: - збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо); - некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо); - навмисні дії сторонніх осіб

(несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1С, спричинення витоку інформації); - помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо); - навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією). Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи. Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту. Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви: - сторонні, які не знають фірму; - сторонні, які знають фірму, та колишні співробітники; - співробітники-непрограмісти; - співробітники-програмісти. Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс і доступне на піратських CD-ROM, у спеціальних розділах BBS і на сайтах Інтернет та ін. Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники». Хакери (хекери) — це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно

заради задоволення від самого процесу роботи. У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів КС тільки для самоствердження (див. приклад). Останнє відрізняє хакерів від професійних зламувачів — кракерів (або «крекерів»), які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень. Найбільш криміногенною групою є пірати — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв'язку. В усіх випадках мотивація – матеріальні інтереси. За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів. Шкідники (вандали) намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль. Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про експериментаторів («піонерів»). Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законослухняні. Отже, одними з основних причин порушення безпеки інформації є незапитаність творчого потенціалу в поєднанні з неусвідомленням

усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати приводом для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитись і самоствердитись існує ще недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються об'єктом уваги фахівців.

Всі заходи протидії комп’ютерним злочинам, що безпосередньо забезпечують безпеку інформації можна поділити на: - правові; - організаційно-адміністративні; - інженерно-технічні. До правових заходів) слід віднести розробку норм, які встановлюють відповідальність за комп’ютерні злочини, захист авторських прав програмістів, удосконалення карного і цивільного законодавства і судочинства. До них відносяться також питання суспільного контролю за розробниками комп’ютерних і прийняття відповідних міжнародних договорів про обмеження, якщо вони впливають або можуть впливати на військові, економічні і соціальні аспекти країн. В останні роки в Україні з’явилися роботи з проблем правової боротьби з комп’ютерними злочинами і відповідно і вітчизняне законодавство стало на шлях боротьби з комп’ютерною злочинністю. До організаційно-адміністративних заходів відносяться: охорона КС, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки одним спеціалістом, наявність плану відеовлення працездатності об’єкту (комп’ютерного центру) після виходу його з ладу, обслуговування ОЦ сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення його роботи, універсальність засобів захисту від усіх користувачів, (включаючи вище керівництво), покладання відповідальності на осіб, які повинні забезпечувати безпеку ОЦ, вибір місця розташування ОЦ тощо. До інженерно-технічних заходів, які подані на рисунку 2.7, можна віднести захист

від несанкціонованого доступу до КС, резервування важливих комп'ютерних блоків і систем, резервне електроживлення, розробку та реалізацію спеціальних програмних і апаратних комплексі тощо.

Фізичні засоби містять у собі різні інженерні засоби, які перешкоджають фізичному проникненню зловмисників на об'єкти захисту, які захищають персонал, матеріальні засоби і фінанси, інформацію про протиправні дії.

Програмні засоби – це спеціальні програми, програмні комплекси і системи захисту інформації в КС (інформаційних системах) різного призначення і засобах обробки даних.

Криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, яка передана (передається) по каналах зв'язку, збереженої та опрацьованої на комп'ютерах з використанням методів шифрування.

3.1 Засоби захисту інформації

Мал.3.

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об’єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту. Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням комп’ютерів, мереж і т. ін. Ці норми здебільшого не є обов’язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США. Правові засоби захисту - чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання. Перехід до інформаційного суспільства вимагає удосконалення використання ІТ.карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об’єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проекту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи, було внесено зміни, оскільки його розцінили як такий, що суперечить положенням про права людини і надає урядам і поліцейським органам зайві повноваження. Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування ІС, використання її ресурсів, діяльність

персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки. Вони охоплюють: - заходи, які передбачаються під час проектування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.); - заходи, що здійснюються під час проектування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо); - заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань і т. ін.); - розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо). Адміністративні засоби є неодмінною частиною захисту інформації. Їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації, а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються). Засоби фізичного (технічного) захисту інформації - це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів ІС, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять: - засоби захисту кабельної системи. За

даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи (СКС), в якій використовуються однакові кабелі для організації передавання даних в ІС, сигналів від датчиків пожежної безпеки, відеоінформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів; - засоби захисту системи електроживлення. Американські дослідники з компанії Best Power після п'яти років досліджень проблем електроживлення зробили висновок: на кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності ІС можливе використання аварійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій; - засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті); - засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо. До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв

інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи і предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього. Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними. Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо. Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Сучасним прикладом є випадок роздрукування на друкуючих пристроях комп'ютерів компконтрактів з малопомітними викривленнями обрисів окремих символів тексту - так вносилась шифрована інформація про умови складання контракту. Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіоі відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений. Щодо впровадження засобів програмно-технічного захисту в ІС, розрізняють два основні його способи: 1) додатковий захист - засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;

2) вбудований захист - механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи. Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

3.2 Методи і системи захисту інформації

Функції і завдання захисту інформації визначають склад і структуру методів і систем захисту. Перелік основних методів захисту інформації поданий на рисунку.

Мал.4. Методи захисту інформації комерційного підприємства

Одним із основних видів загроз цілісності і конфідеційності інформації, а також працездатності КС є навмисні загрози, реалізація яких заздалегідь планується зловмисником для нанесення шкоди.

Даний суб'єктивізм безпосередньої реалізації можна розділити на дві групи:

- загрози, реалізація яких здійснюється при постійній участі людини (зловмисника);
- загрози, реалізація яких здійснюється відповідними комп'ютерними програмами без безпосередньої участі людини.

Завдання захисту від загроз кожного з цих типів однакові і полягають в наступному:

- унуможливення несанкціонованого доступу до ресурсів комп'ютерних систем;
- унеможливення несанкціонованого використання комп'ютерних ресурсів, якщо доступ до них все-таки здійснений;
- своєчасно виявити факт несанкціонованих дій і усунути причини, а також наслідки їх реалізації.

Способи вирішення перерахованих завдань захисту від несанкціованих дій з боку людей і комп'ютерних програм суттєво відрізняються один від одного. Основні функції системи захисту полягають в тому, що перепони несанкціонованого доступу людей до ресурсів КС полягають перш за все в ідентифікації та підтвердженні достовірності користувачів при доступі в КС , а також розмежуванні їх доступу до комп'ютерних ресурсів. Важливою є також функція коректного завершення сеансу роботи користувачів, що запобігає можливості реалізації загрози маскування під санкіонного користувача КС. Захист інформації від дослідження і копіювання передбачає криптографічний захист даних, які захищаються, і виконується шляхом їх шифрування. Крім того, має бути передбачене знищення залишкової інформації, а також аварійне знищення даних. Захист програм від копіювання запобігає можливості виконання несанкціоновано скопійованої програми на іншому комп'ютері. Захист програм від дослідження дозволяє захистити від дослідження алгоритмічні і інші деталі реалізації програми.

Системою захисту стосовно будь-якого користувача мають бути передбачені наступні етапи допуску до комп’ютерної (обчислювальної) системи:

- ідентифікація;
- встановлення достовірності (аутентифікація);
- визначення повноважень для подальшого контролю і розмежування доступу до комп’ютерних ресурсів.

Ці етапи повинні виконуватися і при підключенні до КС таких пристроїв, як віддалені робочі станції і термінали.

3.3 Процес захисту інформації

Як показує практика, несанкціонований доступ є однією з найсерйозніших загроз для зловмисного заволодіння інформацією, що захищається, в сучасних КС. Для ПК небезпека цієї загрози в порівнянні з великими комп'ютерами збільшується, чому сприяють наступні об'єктивно існуючі обставини: - переважна частина ПК розташовується безпосередньо в робочих кімнатах фахівців, що створює сприятливі умови для доступу до них сторонніх осіб; - багато ПК служать колективним засобом опрацювання інформації, що знеособлює відповідальність, у тому числі і за захист інформації; - сучасні ПК оснащені накопичувачами на жорстких дисках дуже великої ємності; -зовнішні накопичувачі виробляються в такій масовій кількості, що вже давно використовуються для поширення інформації так само, як і паперові носії; - спочатку ПК створювалися саме як персональний засіб автоматизації опрацьовання інформації, а тому і не оснащувалися спеціально засобами захисту від несанкціонованого доступу.

Основними механізмами захисту ПК від несанкціонованого доступу є наступні:

- фізичний захист ПК і носіїв інформації;
- розпізнавання (аутентифікація) користувачів та компонентів інформації;

- розмежування доступу до елементів інформації;
- криптографічний захист інформації, яка зберігається на насіях;
- криптографічний захист інформації в процесі її опрацювання;
- реєстрація всіх звернень до інформації, що захищається.

Аутентифікація (розпізнавання) користувачів в ПК не має принципових відмінностей від тих способів, що вже були розглянуті.

Для розпізнавання компонентів опрацювання даних, тобто ПК, ОС, програм функціонального опрацювання, масивів даних (таке розпізнавання особливо актуальне при роботі в комп'ютерній мережі), використовуються наступні засоби: - спеціальні апаратні блоки-приставки (для розпізнавання комп'ютера, терміналів, зовнішніх пристроїв);
- спеціальні програми, що реалізують процедуру «запит-відповідь»;
- контрольні суми (для розпізнавання програм і масивів даних).

Розпізнавання за допомогою блоків-приставок полягає в тому, що технічні засоби оснащуються спеціальними пристроями, які генерують спеціальні індивідуальні сигнали.

З метою попередження перехоплення цих сигналів і подальшого їх використання, вони можуть передаватися в зашифрованому вигляді, причому періодично може змінюватися не лише ключ шифрування, але і використовуваний спосіб (алгоритм) криптографічного перетворення. Розпізнавання за контрольною сумою полягає в тому, що для програм і масивів даних завчасно обчислюються їх контрольні суми (або інші величини, залежні від змісту ідентифікованих об’єктів). Захист від комп’ютерних вірусів та інших програмних дій є окремим напрямком захисту процесів опрацювання інформації в ПК, комп’ютерних та інформаційних системах.

4. Економічні розрахунки

Метою даних розрахунків є обчислення вартості виконання науково-дослідної роботи «Розробка методів та засобів захисту інформації комерційного підприємства від несанкціонованого доступу». 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 5.1.

Розподіл робіт по етапах і видах виконавців.

Таблиця 5.1.

Етап проведення НДР	**Вигляд робіт**	**Посада виконавця**
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР «Розробка методів та засобів захисту інформації комерційного підприємства від несанкціонованого доступу»	Дипломник, керівник
	1. Збір і вивчення науково-технічної	

Вибір напряму дослідження	літератури. 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР . 3. Вибір напряму проведення досліджень для подальшої розробки. 4. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник
Теоретичні і експериментальні дослідження	Інформаційні системи комерційного підприємства 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 5.2.

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР «Розробка методів та засобів захисту інформації комерційного підприємства від несанкціонованого доступу»	**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 подальшої розробки.	**2**
5. Огляд технології захисту комп'ютерних систем	**5**
6. Програмні засоби інформаційної системи комерційного підприємства	**3**
7. Програмне забезпечення комерційного підприємства	**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:

Здер= 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 5.3.

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 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 5.4.

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:

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

Цр = 17373,51грн.

5. Охорона праці

Розділ “Охорона праці”

1. Вступ
2. Аналіз та забезпечення безпеки умов праці.

2.1. Організація робочого місця.

2.2. Основні вимоги безпеки до мікроклімату виробничих приміщень, освітлення

2.3. Шум, вібрація, ультразвук, інфразвук.

2.4. Електробезпека

3. Пожежна безпека
4. Висновок.

1.Вступ

Умови та безпека праці, їх стан та покращення – самостійна і важлива задача соціальної політики будь-якої сучасної промислово розвинутої держави, яку вирішує така невід'ємна складова БЖД, як охорона праці. Рівень безпеки будь-яких робіт у суспільному виробництві значною мірою залежить від рівня правового забезпечення цих питань, тобто від якості та повноти викладення відповідних вимог в законах та інших нормативно-правових актах. Для вирішення існуючих проблем в сфері охорони праці необхідна ефективна взаємодія всіх органів державної влади та громадськості, а також реалізація як на державному, так і на місцевих рівнях відповідних програм, спрямованих на корінне покращення умов і охорони праці.

Законодавство України про охорону праці – це система взаємопов'язаних нормативно-правових актів, що регулюють відносини у сфері соціального захисту громадян у процесі трудової діяльності. Базується законодавство України про охорону праці на конституційному праві всіх громадян України на належні, безпечні і здорові умови праці, гарантовані статтею 43 Конституції України.

Основоположним документом в галузі охорони праці є Закон України «Про охорону праці», який визначає основні положення щодо реалізації права на охорону життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні.

2. Аналіз та забезпечення безпеки умов праці

На підприємстві аналіз і оцінка стану умов та безпеки праці здійснюється на підставі наступних загальних показників: - рівень виробничого травматизму; - рівень професійних захворювань пов’язаних з умовами праці; - кількість працівників, що працюють в умовах, які не відповідають санітарно гігієнічним нормам; - кількість обладнання, що не відповідає вимогам нормативних актів про охорону праці; - кількість технологічних процесів, що не відповідають вимогам нормативно правових актів з охорони праці; - кількість будівель та споруд, технічний стан яких не відповідає будівельним нормам і правилам; - забезпечення працівників засобами індивідуального захисту; - забезпеченість працівників санітарно-побутовими приміщеннями; - витрати на покращення стану безпеки, гігієни праці та виробничого середовища; - витрати на відшкодування збитків потерпілим від нещасних випадків та професійних захворювань, що пов’язані з умовами праці; - витрати на розслідування та ліквідацію наслідків аварій, нещасних випадків та професійних захворювань.

2.1. Організація робочого місця

Необхідними вимогами є:

- характеристика робочого місця;
- загальні вимоги до організації робочого місця;
- оснащення робочого місця;
- просторова організація робочого місця та порядок розміщення організаційної оснастки, інструментів, матеріалів;
- опис організації праці на робочому місці та рекомендовані передові прийоми і методи праці;
- організація обслуговування робочого місця, способи і засоби зв'язку зі службами обслуговування й управління;
- умови праці на робочому місці;
- вимоги безпеки і охорони праці;
- нормування праці, застосовувані форми і системи оплати праці;
- документація на робочому місці;
- економічна ефективність від впровадження типового проекту.

2.2. Основні вимоги безпеки до мікроклімату виробничих приміщень, освітлення

Робоче приміщення програміста, має загальну площу 20 м^2, висоту стелі 3 м. У приміщенні знаходиться 7 робочих місць з ПК. Слід відзначити, що площа одного робочого місця оператора ПК не повинна бути меншою за 6м^2, а об'єм не менший за 20м^3 [1], тобто площі та об'єму даного приміщення не вистачає для розташування 7 робочих місць операторів ПК. Забороняється встановлювати комп'ютери в приміщеннях, розташованих у підвалах будівель. Приміщення укомплектоване системами центрального опалення та кондиціонування повітря. Також в приміщенні присутні аптечки першої до медичної допомоги.

Мікроклімат – це сукупність показників робочого місця, які впливають на тепловий обмін працівників з оточуючим середовищем. До них відносяться: температура повітря (ºС), відносна вологість (%), швидкість руху повітря (м/с), інтенсивність теплового випромінювання (Вт/м²), барометричний тиск (мм рт. ст.).

Мікроклімат виробничих приміщень впливає на тепловий стан організму людини, його теплообмін з навколишнім середовищем. Він нормується в залежності від теплових характеристик виробничого приміщення, категорії робіт по важкості і періоду року.

Таблиця 1. Норми мікроклімату для приміщень з ПК

Пора року	Категорія робіт	Температура повітря, °С, не більше	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодна	легка – 1а	22-24	40-60	0,1
	легка – 1б	21-23	40-60	0,1
Тепла	легка – 1а	23-25	40-60	0,1
	легка – 1б	22-24	40-60	0,2

2.3. Шум, вібрація, ультразвук, інфразвук.

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.

Щоб знизити негативний вплив інфразвуку на людину співробітниками інституту розроблені Державні санітарні норми «Допустимі рівні інфразвуку в приміщеннях житлових та громадських будинків та на прилеглих до них територіях».

2.4. Електробезпека

Приміщення лабораторії за небезпекою ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, без пилу, з нормальною температурою повітря, ізольованими підлогами і малим числом заземлених приладів).

На робочому місці програміста з всього устаткування металевим є лише корпус системного блоку комп'ютера, але тут використовуються системні блоки, що відповідають стандартові фірми IBM, у яких крім робочої ізоляції передбачений елемент для заземлення і провід з жилою, що заземлює, для приєднання до джерела живлення.

На протязі роботи на корпусі комп'ютера накопичується статична електрика. На відстані 5-10 см від екрана напруженість електростатичного поля складає 60-280 кВ/м, тобто в 10 разів перевищує норму 20 кВ/м.

Для захисту працівників від ураження електричним струмом використовуються окремо або у поєднанні один із одним такі засоби, як-от: захисне заземлення; захисне занулення; захисне відімкнення; вирівнювання потенціалів; ізоляція струмопровідних частин; забезпечення недоступності неізольованих струмовідних частин; обмеження сили струму; попереджувальні сигналізація, знаки та написи.

3. Пожежна безпека

Пожежна безпека — стан об'єкта, при якому з регламентованою ймовірністю відкидається можливість виникнення та розвиток пожежі, і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей.

До первинних засобів пожежогасіння належать: вогнегасники; ящики з піском; бочки з водою; покривала з негорючого теплоізоляційного матеріалу; пожежні відра, совкові лопати, пожежний інструмент — кирки, сокири, багри, ломи тощо. Найефективнішим первинним засобом пожежогасіння є вогнегасник. Первинні засоби пожежогасіння можна зберігати на пожежних щитах (стендах) червоного кольору, які встановлюють у виробничих, складських, допоміжних приміщеннях, будинках, спорудах, а також на території підприємств.

4. Висновок.

На сучасному етапі розвитку підприємництва в Україні питання, пов’язанні з комерційною таємницею та її захистом, інформаційною безпекою інфраструктури, привертають увагу значної кількості науковців і аналітиків в галузі теорії підприємництва. Інформаційна безпека підприємництва — це невід’ємна складова національної інформаційної безпеки

ПЕРЕЛІК ПОСИЛАНЬ

1. https://uk.wikipedia.org/wiki/Криптографія.
2. http://uareferat.com/.
3. http://ua.textreferat.com/
4. http://soft/compulenta/ru
6. http://litek.ru/catalog/acronis/homeRe.html
7. https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil1.html
8. https://uk.wikipedia.org/wiki/Захист_інформації_в_локальних_мережах
9. https://buklib.net/books/28625/
10. https://pidru4niki.com/1350082645328/politekonomiya/vidi_pidpriyemstv

ЛІТЕРАТУРА

1. Економіка підприємства: підручник для вузів / За ред. проф. В. Я. Горвінкеля, проф. В. А. Швандар. -М: ЮНІТА-ДАНА, 2001.

2. Агаєв В. С. Конкуренція: аналіз, стратегія, практика. -М., 1996.

3. Брєддік У. Менеджмент організації. -М: Інфра-М, 1997.

4. Грузінов В. П. Економіка підприємства та підприємництва. -М: Софіт, 1999.

5. Лапуста М. Г. Мале підприємництво. - М: Інфра-М, 1997.

6. Ліпсіц І. В. Комерційне ціноутворення. - М.: Бек, 1997.

7. Інформатика / Курносов А.П., Кульов С.А., Улезько А.В. та ін; під ред А.П. Курносова. - М.: Колос, 2005.

8. Комп'ютерні мережі та засоби захисту інформації: Навчальний посібник / Камалян А.К., Кульов С.А., Назаренко К.М., Ломакін С.В., Кусмагамбетов С.М.; Під ред. д.е.н., професора А.К. Камалян. - Воронеж: ВДАУ, 2003.

9. Леонтьєв В. П. Новітня енциклопедія персонального комп'ютера 2005. - М.: ОЛМА-ПРЕСС Освіта, 2005.

10. Черняков М.В., Петрушин А.С. Основи інформаційних технологій. Підручник для вузів: - М.: ИКЦ «Академкнига», 2007.