**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ХАРЧОВИХ ТЕХНОЛОГІЙ**

*Кафедра інформаційних технологій та кібербезпеки*

**Реферат**

по дисципліні

«**Цивільна Оборона**»

«**»**

Виконав Баштовий О.В

Група 353м

Дата здачі реферату“\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2013

Перевірили:

\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Одеса - 2013**

**ВСТУП**

Загально прийнято , що розвиток цивілізації тісно пов'язаний з інформатизацією суспільства. Зростаючі потоки інформації є наслідком розвитку суспільства і , в свою чергу , істотно впливають на його подальше просування .

Тяга до знань , до отримання все нових порцій інформації притаманне людині , а його право на отримання інформації знайшло своє відображення в міжнародному законодавстві . У « Декларації прав і свобод людини і громадянина» , ратифікованої Верховною Радою України .

Чому ж тоді треба захищати інформацію? Зауважимо , по перше , що всі великі обсяги інформації обробляються за допомогою автоматизованих систем обробки інформації. Складність таких систем зростає. Разом з тим ряд збоїв або відмов у функціонуванні таких систем можуть призвести до знищення інформації або її спотворення . Так , наприклад , вихід з ладу накопичувача на жорсткому магнітному диску файлового сервера автоматизованої системи при роботі з інформацією банку може привести до катастрофічних наслідків , якщо не було вжито заходів по збереженню зберігалася на диску інформації.

Однак центральне місце в проблемі захисту інформації займає навмисна діяльність людей, пов'язана з маніпуляцією інформацією , що зберігається і оброблюваної в автоматизованих системах в умовах безконтрольного допуску до неї. У першу чергу це відноситься до випадків комп'ютерних злочинів , пов'язаних з корисливим використанням та спотворенням інформації , нав'язуванням помилкових повідомлень . Ряд інших, що виникають тут проблем , проілюструємо прикладами.

Іншим моментом , пов'язаним з комп'ютерними злочинами , є порушення авторських прав на програмне забезпечення. Проблема незаконного копіювання та використання програмного забезпечення характерна не тільки для України. Частка " піратського " ​​програмного продукту в загальному обсязі використовуваного програмного забезпечення (ПО) коливається від 50 % у розвинених країнах до 05 % - в нерозвинених . За наявними оцінками збитки від несанкціонованого копіювання програм становлять в США близько 50 % від вартості загального ринку про грам . Для нас ця проблема важлива тим , що широке використання незаконно придбаного програмного забезпечення підриває вітчизняну індустрію програмного забезпечення.

Для характеристики стану справи у нас в України обмежимося тільки оцінкою Голови гостя комісії при Президентові України: «... Відсталість інформаційних технологій , що не забезпечують захист інформації , висока скритність злочинів , скоєних за допомогою комп'ютерних засобів , складність їх докази , створюють сприятливі умови для розвитку в України інформаційної злочинності . Як показали перевірки банків , вже в

Загальний збиток від них склав кілька десятків мільярдів гривень і має стійку тенденцію до подальшого зростання ».

Наведені приклади відносяться хоча і до недалекого , але минулого. За минулий час можна було врахувати уроки того, що відбулося і вжити заходів , що запобігають несанкціонованому доступу до інформації , що зберігається і оброблюваної в обчислювальних системах . Однак ситуація не стає істотно кращою .

З викладеного випливає, що для забезпечення нормального функціонування інформаційних систем всіх рівнів необхідно потурбуватися про те, як:

• Запобігти руйнівного вторгнення в систему;

• із загального обсягу зберігається та обробляється інформації виділити деяку частину її, яка не повинна бути загальнодоступною;

• Своєчасно і в повному обсязі забезпечити пре доставляння необхідної інформації законному користувачеві.

Поряд з названими проблемами, вирішення яких забезпечує захист інформації, останнім часом все більша увага приділяється також проблемам захисту користувача від "шкідливої ​" інформації. Шкідливі впливу на користувача можуть носити різний характер. Говорячи, наприклад, про вплив "віртуальної реальності" на психіку людини, мають на увазі деякі недосліджені технічні та медичні аспекти . На іншому полюсі стоять проблеми , пов'язані зі зловмисними або корисливі ми устремліннями деяких представників суспільства. Сюди можна віднести брехливу рекламу, пропаганду насильства, і т.п.

Поняття "захист інформації" та "захист від інформації" акумулюють у собі поняття " інформаційна безпека".

Інформація та інформаційні процеси стали невід'ємною частиною життя особистості , суспільства і держави , а інформаційна безпека значущою складовою національної безпеки .

1 . **ВІД ЧОГО ТРЕБА ЗАХИЩАТИ ІНФОРМАЦІЮ**

Для того щоб сформулювати завдання захисту інформації від зловмисників , необхідно перед ставити собі їх цілі і можливості по досягненню цих цілей.

Зазвичай розрізняють наступні цілі порушника :

• незаконне заволодіння конфіденційною інформацією;

• спотворення інформації;

• знищення інформації;

• порушення функціонування АС ;

• незаконне копіювання програм (і другої цінної інформації);

• відмова від інформації.

Під конфіденційною інформацією будемо розуміти інформацію, доступ до якої обмежується відповідно до законодавства.

факт потрапляння такої інформації зловмиснику називають витоком інформації і говорять про захист інформації від витоку. Витік інформації може бути різною за наслідками. Так , наприклад , витік інформації , пов'язана з розкраданням носія або навіть комп'ютера в цілому , дуже швидко виявляється. Водночас негласна для законного власника витік інформації завдає більшої шкоди .

Спотворення інформації також може бути явним або неявним для власника інформації. Якщо, наприклад , зловмисник перехопив ( шифрування ) повідомлення і не може дізнатися його змісту , він може довільно спотворити частину тексту. Швидше за все , одержувач виявить таке спотворення і зробить заходи з виправлення ситуації. Неявне спотворення інформації називають модифікацією. Модифікація інформації може проявлятися по різному. На приклад, у фінансовому документі вона може полягати в " виправленні " номера рахунку, куди треба пере слати гроші , або розміру суми, що підлягає перерахуванню за вказаною адресою. У мережах з комутацією пакетів модифікація може полягати у вилученні з каналу зв'язку частині повідомлення, зміна по рядка проходження частин повідомлення. Нарешті, можливий повтор або посилка фальсифікованого повідомлення, наприклад, із зазначенням банку перерахувати гроші.

Знищення інформації може привести до краху обчислювальної системи, якщо не були прийняті профілактичні заходи з резервного копіювання інформації, і до тимчасового виходу системи з ладу при наявності резервних копій.

Під порушенням функціонування автоматизованої системи мають на увазі (на відміну від знищення інформації) потайні дії , що заважають нормально функціонувати системі . Наслідком такого порушення може бути неподання інформації законному користувачеві. Порушення функціонування АС можуть здійснюватися захопленням ресурсів , запуску на рішення сторонніх завдань або підвищенням пріоритетності завдань, які потребують термінового вирішення . До зазначених втручань в роботу найбільш чутливі інформаційні системи, що працюють в режимі реального часу або в режимі оперативного прийняття рішень.

2 . УРАЗЛИВІ МІСЦЯ АВТОМАТИЗОВАНИХ СИСТЕМАХ І МЕРЕЖАХ

Перераховуючи вразливі місця автоматизованих систем і мереж з точки зору захисту інформації , ми змушені будемо перерахувати практично всі елементи , їх складові.

1 . Розглянемо окрему автоматизовану систему, що представляє собою окремий комп'ютер або локально обчислювальну мережу. Іноді для стислості будемо називати її просто системою .

Якщо зловмисник отримав доступ до комп'ютера з захищається інформацією, то він може її скопіювати , змінити або знищити . Крім того , порушник може вивести комп'ютер з ладу або почати дії з порушення функціонування автоматизованої системи , елементом якої він є.

При наявності в автоматизованій системі інформації обмеженого доступу для її захисту зазвичай сформулюються і реалізуються правила розмежування доступу. Втім , відповідно до закону "Про інформацію , інформатизації і захисту інформації" захисті, (щонайменше - захисту від знищення ) , повинна підлягати будь-яка інформація , що входить до складу інформаційного ресурсу , або яка є власністю або товаром. Тому правила розмежування доступу повинні бути сформульовані завжди . Їх мінімальним вмістом має бути розрізнення користувачів за принципом " свій - чужий". Дії зловмисника з отримання доступу до інформації в обхід правил розмежування доступу ( з використанням тільки штатних засобів обчислювальної системи ) носять назву несанкціонованого доступу.

2 . Розглянемо тепер автоматизовану систему у складі телекомунікаційної мережі. Навіть якщо вона захищена від несанкціонованого доступу до інформації , вона може бути вразлива від зловмисника , що має віддалений доступ. Більш того , віддалений доступ може принести більшої шкоди , ніж несанкціонований доступ усередині системи.

Справа в тому , що в розглянутому випадку зловмисник може витратити на дослідження можливості проникнення в систему значний час і залишатися при цьому анонімним.

В результаті проникнення він може досягти тих же цілей , що і при локальному несанкціонованому доступі: витоку , спотворення і / або знищення інформації . Він може спробувати порушити функціонування системи , запустивши рішення своєї , бути може безглуздою завдання, що вимагає всіх або майже всіх ресурсів системи . Іншими способами порушення функціонування системи можуть бути організація потоку запитів , критичного за обсягом для системи, або запуск вірусу або хробака. Нарешті , саме в умовах віддаленого доступу можлива відмова від факту відправлення або факту отримання повідомлення.

3 . Дуже вразливі мережі в разі отримання зловмисником доступу до вузла зв'язку , а також при підключенні до комутаційного обладнання . У цих випадках зловмисник отримує можливість :

• зчитувати і модифікувати інформацію , про що ходить через точку підключення;

• блокувати проходження інформації;

• записувати і посилати повідомлення повторно ;

• створювати і посилати свої повідомлення , маскуючи їх під повідомлення законних користувачів;

• спостерігати трафік ( інтенсивність і обсяги обміну інформацією , напрямку передачі інформації).

4 . Приблизно такі ж можливості є у зловмисника , що підключився до каналу зв'язку . Однак сама така можливість підключення залежить від

фізичної природи каналу. Найбільш чутливі до перехоплення інформації радіоканали і, в тому числі , канали супутникового зв'язку. Підключення до ка налу зв'язку в цьому випадку проводиться з використанням антени і зв'язкового обладнання . Підключення залишається практично непомітним для законних користувачів мережі.

Знімання інформації з кабельних каналів , навіть оптоволоконних , також можливий , хоча й більш складний, ніж у випадку використання радіоканалів .

5 . Комп'ютер і його складові частини: системний блок , дисплей , клавіатура - є елементами електронного обладнання. Відбуваються в них фізичні процеси під час функціонування , при водять до виникнення змінних електромагнітних полів. Зазначені поля можуть нести в собі захищається інформацію обмеженого доступу. Ця інформація може уловлюватися спеціальними прийомними пристроями на деякому віддаленні від комп'ютера. У даному випадку говорять про вразливість від паразитних електромагнітних випромінювань .

За певних умов витік інформації може бути організована по акустичному , оптичному , вібраційному каналам. У загальному випадку говорять про уразливість до витоку інформації технічними каналами витоку.

3 . **НАПРЯМКИ ЗАХИСТУ ІНФОРМАЦІЇ**

Аналіз вразливих місць автоматизованих систем обробки інформації , а також можливостей зловмисника по впливу на автоматизовану систему , дає можливість виділити кілька відносно самостійних напрямків захисту інформації. До них відносяться:

• законодавче забезпечення захисту інформації;

• захист інформації від несанкціонованого до ступа ;

• розвиток і використання криптографічних методів захисту інформації;

• захист інформації від комп'ютерних вірусів і інших небезпечних впливів по каналах розповсюдження програм ;

• захист від несанкціонованого копіювання та розповсюдження програм і цінної комп'ютерної інформації;

• захист конфіденційної інформації від витоку каналами побічних електромагнітних випромінювань і наведень ;

• захист інформації в надзвичайних ситуаціях і при несправності апаратної частини АС .

**3.1 . ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ .**

Чинним законодавством України визначається правовий статус інформації , конституційні права громадян у галузі інформаційної безпеки , правові основи захисту інформації обмеженого доступу і захисту інтелектуальної власності.

Ряд підзаконних нормативних документів визначає системи ліцензування діяльності з за щиті інформації та сертифікації засобів захисту інформації. Зважаючи на виняткову важливість інформації та інформатизації для розвитку суспільства і держави.

**3.2 . ЗАХИСТ ІНФОРМАЦІЇ Від несанкціонованого доступу**

Захист інформації від НСД вирішує наступні завдання [12]:

• захист інформації обмеженого доступу від витоку ;

• захист інформації від спотворення (забезпечення цілісності інформації);

• захист автоматизованої системи від спроб порушення її функціонування.

У частині технічної реалізації захист від НСД зводиться до задачі розмежування функціональних повноважень і доступу до інформації.

Найпростіший спосіб захисту автоматизованої системи від віддаленого доступу несанкціонованих користувачів - це відмова від роботи в мережі , забезпечення фізичного захисту від усіх зовнішніх мережевих з'єднань. У найбільш відповідальних випадках так і роблять.

Організація захисту інформації від НСД передбачає наявність механізмів аутентифікації ( підтвердження автентичності ) :

  суб'єкта доступу ( локального або віддаленого ) ;

  змісту одержуваного повідомлення;

  поточного сеансу зв'язку.

Найбільш відомою системою аутентифікації суб'єкта локального доступу є парольний система .. Існуюче різноманіття програмно -апаратних засобів аутентифікації вимагають використання аутентифікатор , що представляють собою або якийсь особистий секрет (наприклад ключова дискета , електронний ключ ), або унікальний не підробляв ознака (наприклад , відбиток пальця , райдужна оболонка ока) .

У разі віддаленого доступу для аутентифікації відправника , змісту повідомлення і сеансу зв'язку найчастіше використовується електронний цифровий підпис.

Суб'єкт доступу , що успішно пройшов етап аутентифікації отримує доступ до ресурсів відповідно до правил розмежування доступу. Правила розмежування доступу повинні чітко вказувати кожному суб'єкту доступа об'єкти, доступні для нього (файли, папки , тощо) та права на їх використання : створювати , читати , редагувати , видаляти , і т.п.

3.3 . **Використання криптографічних методів ЗАХИСТУ ІНФОРМАЦІЇ**

Стержень будь-якої системи захисту - криптографічні засоби .

Як наука , а іноді і як мистецтво шифрування повідомлень , криптографія має багатовікову історію. Розвиток комп'ютерних систем телекомунікацій , необхідність вирішення завдань аутентифікації і ряду інших завдань , пов'язаних із забезпеченням юридичної значимості електронних документів та захистом від відмов привели останнім часом до розвитку нових напрямків у криптографії , пов'язаних з вирішенням такого роду завдань [ 6 , 14 ] .

1 . Під шифруванням інформації розуміють таке її перетворення , при якому супротивник або зловмисник , отримавши доступ до такої перетвореної інформації , не зможе нічого зрозуміти .

Система шифрованого обміну інформацією ви дивиться в такий спосіб. Відправник повідомлення шифрує відкритий текст на деякій секретному ключі , отримує шифрований текст , або крипто граму , і посилає її по каналу зв'язку. Одержувач на деякій секретному ключі розшифровує шифрований текст і отримує відкритий текст повідомлення. Третя зацікавлена ​​сторона - противник , або зловмисник , перехопивши криптограму , намагається дешифрувати її , тобто визначити тим чи іншим способом відкритий текст повідомлення або секретний ключ.

2 . Всі криптографічні системи поділяються на два класи .

Класичні або симетричні системи , характеризуються тим , що ключ для зашифрування збігається з ключем розшифрування , і, отже , є секретним . Однаковими ключами відправника і одержувача , як правило , постачає третя сторона - служба генерації та розсилки ключів.

Асиметричні криптосистеми виникли з потреби організації шифрованого обміну інформацією в мережах ЕОМ в умовах відсутності служб централізованого виготовлення та розсилки ключів. При використанні асиметричної системи потенційний одержувач секретної інформації вибирає (або обчислює за відомим алгоритмом ) ключ , який тримає в секреті і буде використовувати його для розшифрування одержуваних їм повідомлень . Так леї, він обчислює парний секретному ключ для зашифрування повідомлень. Цей ключ не є секретним , оголошується загальнодоступним ( public key ) , і публікується або розсилається передбачуваним отруйникам повідомлень.

Асиметричні шифри працюють з помітним уповільненням в порівнянні з симетричними шифрами . Тому в даний час найбільш перспективним представляються рішення, пов'язані з гібридними крипто схеми , що використовують традиційні методи шифрування з секретним ключем для захисту секретності і цілісності , при одночасному використанні методів шифрування з відкритим ключем для реалізації функцій розподілу ключів.

Використання симетричних криптографічних систем дозволяють вирішувати проблеми автентифікації і забезпечення цілісності повідомлення. Автентифікація відправника досягається самим фактом отримання повідомлення , зашифрованого на ключі , відомому тільки відправнику. Перевірка цілісності повідомлення забезпечується додаванням в текст криптограми деякої додаткової інформації, що грає роль контрольної суми. Контрольна сума є функцією всього повідомлення і секретного ключа. Цілісність повідомлення підтверджується збігом значень контрольної суми , обчисленої на передавальному і приймальному кінцях .

Описана система підтвердження цілісності повідомлення добре працює в умовах взаємодовіри серед учасників обміну . Для автентифікації інформації за відсутності взаємної довіри між учасниками інформаційного обміну Діффі і Хелманом в 176 році була запропонована концепція

« Цифровий підпис». [ 13 ] Вона полягає у використанні асиметричних криптосистем для автентифікації інформації.

Цифровий підпис обчислюється на основі тексту підписувано го повідомлення і секретного особистого ключа. Всякий бажаючий переконатися в достовірності повідомлення використовує для цього як перевірочної комбінації загальнодоступний ключ. При цьому знання перевірочної комбінації не дає можливості підробити підпис.

Таким чином , складовими частинами , що забезпечують реалізацію цифрового підпису є:

• генерація секретного ключа за допомогою датчика випадкових ключів;

* вироблення і опублікування відкритого ключа;
* формування підпису;
* перевірка підпису.

Найважливішою характеристикою використовуваних криптографічних систем є їх стійкість , визначальна впевненість у тому , що передбачуваний зловмисник , який не має доступу до використовуваному криптографічному ключу , не зможе де шифрувати і зрозуміти сенс перехопленою шифрованого інформації, або імітувати підпис хоча б одного повідомлення. Проведення досліджень, що дозволяють отримати таку оцінку, є досить трудомістким і дорогим справою , посильним тільки професійним криптографії. Тому на практиці рекомендується використовувати тільки сертифіковані криптографічні засоби , про які йшли всебічні дослідження та атестацію ФАПСИ . Як приклад гарантовано стій кого алгоритму шифрування можна привести алгоритм по ГОСТ 281478

**3.4 . ЗАХИСТ ВІД ВІРУСІВ**

Захист інформації від комп'ютерних вірусів і інших небезпечних впливів по каналах розповсюдження програм актуальна зважаючи на великі масштабів

« Вірусних епідемій » , при яких заражаються сотні тисяч комп'ютерів .

Останнім часом все частіше серед фахівців згадують про інформаційний зброю. Одним з елементів такої зброї є впровадження в захищаються системи спеціальних програм , званих програмними закладками. Такі закладки можуть бути націлені на нейтралізацію штатних засобів захисту від НСД, порушення функціонування автоматизованої системи , копіюванні і негласної передачі, як смислової інформації (даних) , так і паролів.

Як правило , розглядаються два напрями в методах захисту від програм з шкідливим впливом [ 15 , 16 ] :

• застосування « імуно-стійких » програмних засобів , захищених від можливості несанкціонованої модифікації (розмежування доступу , методи самоконтролю і самовідновлення ) ;

• застосування спеціальних програм аналізаторів , що здійснюють постійний контроль виникнення « аномалій » у діяльності прикладних програм , періодичну перевірку наявності інших можливих слідів вірусної активності ( на приклад , виявлення порушень цілісності програмного забезпечення) , а також «вхідний» контроль нових програм перед їх використанням (за характерними ознаками наявності в їх тілі вірусних утворень ) .

3.5 **. ЗАХИСТ ПРОГРАМ ВІД несанкціонованого копіювання та використання**

1 . Захист від несанкціонованого копіювання та розповсюдження програм і цінної комп'ютерної інформації орієнтована на проблему охорони інтелектуальної власності , втіленої у вигляді програм і цінних баз даних. Такий захист зазвичай здійснюється за допомогою спеціальних програмних та / або програмно -апаратних засобів , що роблять непрацездатною нелегальну копію програми

Програми , поширювані на комерційній основі , поставляються на змінних дисках. Рідше - встановлюються постачальником на конкретний комп'ютер. Ідея , що реалізує захист від несанкціонованого копіювання полягає в тому , щоб створити такий дистрибутив , що копія з нього , одержувана штатними засобами операційної системи , була б непрацездатною. Для цього на дискеті крім блоку з захищається інформацією розміщується блок не дублюється, оригінальної інформації . Під час запуску програми та / або її роботи відбувається звернення до НЕ дубльованих блоку. При цьому ще один блок програмного забезпечення - блок порівняння , переконується в наявності або відсутності блоку не дублюється, інформації. За результатами порівняння або подається команда на продовження роботи захищається програми, або управління передається на блок реагування. Як варіанти реакції в останньому випадку можуть бути команди припинення роботи програми , самознищення захищається програмного продукту і навіть деструктивного віз дії на програмну середу комп'ютера.

Найбільше число методів створіння не копіюються модулів пов'язано з нестандартним форматуванням дискет. Нестандартне форматування здійснюється спеціальними контролерами .

2. Широке поширення отримали програм але апаратні засоби захисту від несанкціонованого копіювання з використанням електронних ключів.

Електронні ключі - це компактні пристрої , які підключаються до одного з зовнішніх роз'ємів комп'ютера , «прозорі» для периферійних пристроїв і грають роль блоку не дублюється, оригінальної інформації . Для реалізації цієї мети електронні ключі виконуються зі значними функціональними можливостями, що включають в себе можливість зміни внутрішнього зі стояння. Через один роз'єм можна підключити не скільки електронних ключів , кожен з яких забезпечує захист своєї програми. Одночасно, але через цей роз'їм може здійснюватися інтерфейс з принтером .

3 . Протидія відновленню алгоритмів . При неможливості отримання несанкціонованої копії захищається дискети досить прості ми методами зловмисник може спробувати відновити захищається програму або алгоритм , реалізуємий захищається програмою. Відновлення програми або алгоритму можливо двома способу ми. Перший з них пов'язаний з аналізом і подальшим дісассемблірованіем роздруківки всього програмного забезпечення , наявного на дискеті.

4 . Проблемі захисту дискет від несанкціонованого копіювання присвячена численна література . Створено також значне число програмних та програмно-апаратних засобів захисту від несанкціонованого копіювання. Однак треба зазначити , що надійного рішення цієї проблеми немає. Будь захист від несанкціонованого копіювання розкривається в кінцевий час.

**3.6 . ЗАХИСТ ІНФОРМАЦІЇ ВІД витоку технічними каналами**

Даний напрямок базується на запобіганні або суттєвому утрудненні можливості отримання порушником інформації обмеженого доступу по каналах паразитних електромагнітних випромінювань і наведень, акустичним і іншим технічним каналам за межі території, що охороняється . При цьому передбачається , що всередині території, що охороняється застосовуються ефективні режимні заходи, що виключають можливість безконтрольного використання спеціальної апаратури пере хвата , реєстрації та відображення електромагнітних сигналів. Для захисту від ПЕМВН широко використовуються екранування приміщень , а також технічні заходи, що дозволяють знизити інтенсивність інформативних випромінювань самого обладнання ЕОМ і зв'язку . Останнім часом певного поширення отримав метод електромагнітної маскування інформативних сигналів.

У деяких відповідальних випадках необхідна додаткова перевірка обчислювального устаткування на предмет можливого виявлення спеціальних закладних пристроїв промислового шпигунства , які можуть бути впроваджені недобросовісним конкурентом з метою ретрансляції або запису інформативних випромінювань комп'ютера , а також мовних і інших несучих вразливу інформацію сигналів [ 21 ] .

**3.7 ЗАХИСТ ІНФОРМАЦІЇ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ І ПРИ НЕСПРАВНОСТІ АПАРАТНОЇ ЧАСТИНИ АС**

1 . Надзвичайні ситуації можуть виникнути в результаті стихійних лих (землетруси і т.п. ) , техногенних катастроф (пожежі , вибухи і т.п.) , терористичних актів та воєнних дій.

Найбільш уразливими об'єктами забезпечення інформаційної безпеки в умовах надзвичайних ситуацій є система прийняття рішень з оперативним діям , пов'язаним з розвитком таких ситуацій , та ходом ліквідації їх по наслідків.

У розглянутих умовах цінність інформації така, що вона повинна залишитися в цілості й доступності при руйнуванні будівлі , обладнання , тощо . Тому велика увага повинна приділятися резервному копіюванню. Резервні копії повинні зберігатися в інших приміщеннях , будівлях , або , навіть , в інших містах .

2 . Перебої з живленням є однією з перших причин втрати інформації в функціонуючої системі. При пропажі живлення , навіть на частки секунди , стирається інформація, що обробляється в енергозалежною оперативної пам'яті. Засобом захисту в розглянутому випадку є використання джерел безперервного живлення .

3. Загрози втрати інформації від збоїв і несправностей апаратної частини АС часто вирішуються випробуваним засобом - дублюванням схильний ної небезпеки частини обладнання.

Близькі за наслідків і загрози, що виникають через помилки в програмному забезпеченні. Нерідкі випадки , коли робота навіть фірмового програмного забезпечення в певних ситуаціях призводить до «зависання » обчислювальної системи . За наступний перезапуск призводить до втрати інформації, що знаходиться в оперативній пам'яті. Підвищенню надійності програмного забезпечення може сприяти ретельне тестування програмного продукту по можливості у всіх режимах його роботи.

4 . Причинами втрати або спотворення інформації , переданої в мережі є:

• збоїв і несправності мережевого обладнання;

• перешкоди в каналі зв'язку .

У локально обчислювальних мережах значна частка загроз за рахунок несправностей в кабельному господарстві . У зв'язку з цим рекомендується мати і використовувати для виявлення факту і місця розриву кабелю або короткого замикання в ньому спеціальні тестери.

Для підвищення надійності передачі інформації в умовах перешкод використовують коди, що виявляють і виправляють помилки .

5 . Недосвідченість користувача , помилки оператора дають значну частку випадків втрати інформації. Сучасне програмне забезпечення , як в рамках операційної системи , так і в спеціальних утилітах , містить засоби, що захищають від помилкового стирання інформації навіть в таких важких випадках, як випадкове форматування дисків.

На Закінчення відзначимо, що при побудові системи ЗАХИСТУ ІНФОРМАЦІЇ необхідній комплексний підхід, який враховує необхідність "закриття" всіх слабких місць обчислювальної системи.

**СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ПРИВАТНОГО ПІДПРИЄМСТВА. ОРГАНІЗАЦІЯ СЛУЖБИ ЗАХИСТУ**

Перед сучасним приватним підприємством гостро стоять проблеми забезпечення інформаційної безпеки.

Це пов'язано з розвитком інформатизації підприємства, з постійно зростаючою вартістю інформації, з

одного боку, і активністю інформаційно-аналітичних структур і різного роду порушників, з іншого.

Інформація обмеженого доступу використовується компаніями-конкурентами, шахраями,

терористами у своїх корисливих цілях, завдаючи збитки підприємству – власникові цієї інформації.

Проблеми й завдання компаній сьогодні стали порівнянні із проблемами й завданнями цілих держав.

Як і держави, вони співробітничають і воюють. Але війни тут називаються інформаційними: хто має

інформацію, володіє якщо не світом, то фінансовими потоками.

Як не дивно, але й сьогодні не всі керівники усвідомлюють нагальну потребу організації на їхньому

підприємстві системи захисту комерційної таємниці. Серед тих, хто таку необхідність все-таки розуміє, чимало не знають, що слід робити, аби зберегти ті чи інші відомості в таємниці, з вигодою реалізувати їх,

не зазнати збитків від їхнього витоку або втрати. Деякі йдуть тільки шляхом оснащення підприємства технічними засобами захисту, повністю ігноруючи організаційно-правові методи. Мається на увазі, зокрема, створення нормативно-правової бази, прийняття й суворе дотримання якої дозволять фірмі не

лише зберегти й використати з вигодою свої секрети, але у разі витоку інформації мати підстави для

подання позовної заяви.

Отже, тільки «комплексна система може гарантувати досягнення максимальної ефективності захисту

інформації, тому що системність забезпечує необхідні складові захисту й установлює між ними логічний і

технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всеохоплення захисту,

забезпечує її надійність».

**Система захисту інформації приватного підприємства**

Метою системи захисту інформації підприємства є:

* запобігання витоку, розкраданню, втраті, перекручуванню, підробці інформації;
* запобігання загрозам безпеці особистості, підприємства, суспільства, держави;
* запобігання несанкціонованим діям щодо знищення, модифікації, перекручування, копіювання,
* блокування інформації;
* запобігання іншим формам незаконного втручання в інформаційні ресурси й системи, забезпечення
* правового режиму документованої інформації як об'єкта власності;
* захист конституційних прав громадян на збереження особистої таємниці й конфіденційності
* персональних даних, що існують в інформаційних системах;
* збереження конфіденційності документованої інформації відповідно до законодавства.

Для грамотної побудови й експлуатації системи захисту необхідно дотримуватись таких принципів

її застосування:

* простота захисту;
* прийнятність захисту для користувачів;
* підконтрольність системи захисту;
* постійний контроль за найбільш важливою інформацією;
* дроблення конфіденційної інформації на складові елементи, доступ до яких мають різні користувачі;
* мінімізація привілеїв доступу до інформації;
* установка пасток для провокування несанкціонованих дій;
* незалежність системи керування для користувачів;
* стійкість захисту в часі й за несприятливих обставин;
* глибина захисту, його дублювання й перекриття;
* особлива персональна відповідальність осіб, що забезпечують безпеку інформації;
* мінімізація загальних механізмів захисту.

Алгоритм створення системи захисту конфіденційної інформації такий:

* визначення об'єктів захисту;
* виявлення загроз і оцінка їхньої ймовірності;
* оцінка можливої шкоди;
* огляд застосовуваних засобів захисту, визначення їхньої недостатності;
* визначення адекватних заходів захисту;
* організаційне, фінансове, юридичне та ін. види забезпечення засобів захисту;
* впровадження засобів захисту;
* контроль;
* моніторинг і коригування впроваджених засобів.

1. Начальник служби захисту інформації призначається наказом керівника підприємства. Він очолює групу компетентних співробітників, які висловлюють свої пропозиції щодо обсягу, рівня й способів забезпечення збереженості конфіденційної інформації.

2. Керівник групи, маючи відповідну кваліфікацію в цій сфері, із залученням окремих фахівців формує попередній список відомостей, які надалі ввійдуть в «Перелік відомостей, що становлять конфіденційну інформацію підприємства».

3. Керівник групи на основі цього списку визначає й подає на узгодження необхідні до захисту.

4. Аналізуються наявні засоби захисту відповідних об'єктів, визначається ступінь їхньої недостатності, неефективності, фізичного й морального зношування.

5. Вивчаються зафіксовані випадки спроб несанкціонованого доступу до захищених інформаційних ресурсів і розголошення інформації.

6. На основі досвіду підприємства, з використанням методу моделювання ситуацій група фахівців виявляє можливі шляхи несанкціонованих дій зі знищення інформації, її копіювання, модифікації, перекручування, використання й т. п. Загрози ранжуються за ступенем значимості й класифікуються за видами впливу.

7. На основі зібраних даних оцінюється можлива шкода підприємству від кожного виду загроз, що стає визначальним фактором для категорування відомостей в «Переліку» за ступенем важливості, наприклад, для службового користування, конфіденційно, суворо конфіденційно.

8. Визначаються сфери обігу кожного виду конфіденційної інформації: за носіями, територією поширення, допущеними користувачами. Для вирішення цього завдання група залучає керівників структурних підрозділів, вивчає їхні побажання.

9. Група проводить підготовку до введення зазначених засобів захисту.

**Література**:

1. Цивільний кодекс України від 16.01.2003 №435-ІV // zakon1.rada.gov.ua.

2. Кодекс України про адміністративні порушення (зі змінами і доповненнями) // Довідник

працівника контрольно-ревізійної служби. – Т. 1. – К.: ДІЯ, 2001. – C. 18–19.

3. Про захист від недобросовісної конкуренції: Закон України від 7.06.1996 №236/96-ВР //

zakon1.rada.gov.ua.

4. Про державну таємницю: Закон України від 21.01.1994 №3855-XII зі змінами та доповнен-

нями від 05.06.2008 / zakon1.rada.gov.ua.

5. Про введення в дію Закону України «Про захист інформації в автоматизованих системах»:

Постанова Верховна Рада України вiд 05.07.1994 №81/94-ВР // zakon1.rada.gov.ua.

6. Про інформацію: Закон України від 02.10.1992 №2657-XII // zakon1.rada.gov.ua.

7. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 368 с.

8. Голубев В.А. Киберпреступность – угрозы и прогнозы // Управління розвитком: Збірник

наукових статей / За ред. В.С. Пономаренко. – №6. – Харків: ХНЕУ, 2008. – С. 103–106.

9. Гуцалюк М.В. Боротьба з комп'ютерною злочинністю як необхідна умова розвитку електронного бізнесу в Україні // www.crime-research.ru