Приходько Олег Олегович,
студент напряму 6.080101 «Геодезія, картографія і землеустрій»
Подільський державний аграрно-технічний університет
м. Кам'янець-Подільський
Науковий керівник: к.е.н., доцент Печенюк А.В.

ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ СУЧАСНОГО ПІДПРИЄМСТВА

Інформація сьогодні перестала бути допоміжним ресурсомвиробництва, а перетворилась у необхідну умову успішного бізнесу. Оскільки роль інформації як виробничого ресурсу постійно зростає, то не можназалишати сферу інформаційного забезпечення управління підприємством без достатньої уваги.Забезпечення безпеки інформації в комп'ютерних мережах передбачає створення перешкод для будь-яких несанкціонованих спроб розкрадання або модифікації даних, переданих у мережі. При цьому дуже важливо зберегти такі властивості інформації, як:доступність,цілісність,конфіденційність

Доступність інформації – здатність забезпечувати своєчасний і безперешкодний доступ користувачів до інформації, яка їх цікавить.Цілісність інформації полягає в її існуванні в неспотвореному вигляді (незмінному стосовно деякого фіксованого її стану).Конфіденційність – це властивість, що вказує на необхідність введення обмежень доступу до даної інформації для визначеного кола користувачів.Неправомірне перекручування, фальсифікація, знищення або розголошення конфіденційної інформації може нанести серйозні, а іноді й непоправні матеріальні або моральні втрати. У цьому випадку, досить важливим є забезпечення безпеки інформації без збитку для інтересів тих, кому вона призначена.

Щоб забезпечити гарантований захист інформації в комп□ютерних системах обробки даних, необхідно, в першу чергу, розглянути і систематизувати всі можливі фактори (загрози), що можуть привести до втрати або перекручування вихідної інформації.Загрози можуть бути як випадковими, так і навмисними.До випадкових загроз відносяться:помилки обслуговуючого персоналу і користувачів;втрата інформації, обумовлена неправильним збереженням архівних даних;випадкове знищення або зміна даних;збої устаткування і електроживлення;збої кабельної системи;перебої електроживлення;збої дискових систем;збої систем архівування даних;збої роботи серверів, робочих станцій, мережевих карт тощо;некоректна робота програмного забезпечення;зміна даних при помилках у програмному забезпеченні;зараження системи комп'ютерними вірусами;несанкціонований доступ;випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.Найчастіше збиток наноситься не через чийсь злий намір, а просто через елементарні помилки користувачів, що випадково псують або видаляють дані, життєво важливі для системи. У зв□язку з цим, крім контролю доступу, необхідним елементом захисту комп□ютерної інформації є розмежування повноважень користувачів.

Надійний засіб запобігання втрат інформації при короткочасному відключенні електроенергії – установка джерел безперебійного живлення (UPS). Різні по своїх технічних і споживчих характеристиках, подібні пристрої можуть забезпечити живлення всієї локальної мережі або окремого комп'ютера упродовж часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітних носіях.

Основний метод захисту інформації і устаткування від стихійних лих (пожеж, землетрусів, повеней тощо) полягає в створенні і збереженні архівних копій даних. Антивірусні програми захищають пристрій від вірусів.

Однак найбільш небезпечним джерелом загроз інформації є навмисні дії зловмисників.Обмеження доступу до ПК шляхом введення кодів не гарантує стовідсотковий захист інформації.Включити комп'ютер і зняти код доступу до системи не вимагає особливих зусиль: досить відключити акумулятор на материнській платі. У крайньому випадку, можна вкрасти системний блок комп'ютера або витягти жорсткий диск і вже в спокійній обстановці одержати доступ до необхідної інформації.

До навмисних загроз відносяться:несанкціонований доступ до інформації і мережевих ресурсів;розкриття і модифікація даних і програм, їх копіювання;розкриття, модифікація або підміна трафіка обчислювальної мережі;розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб;крадіжка магнітних носіїв і розрахункових документів;руйнування архівної інформації або навмисне її знищення;фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому;перехоплення та ознайомлення з інформацією, яка передана по каналах зв□язку тощо.Виділяють три основних види загроз безпеки: загрози розкриття, цілісності і відмови в обслуговуванні.

Спосіб несанкціонованого доступу – це сукупність прийомів і порядок дій з метою одержання (добування) інформації, що охороняється, незаконним протиправним шляхом і забезпечення можливості впливати на цю інформацію (наприклад: підмінити, знищити тощо).При здійсненні несанкціонованого доступу, зловмисник переслідує три мети:одержати необхідну інформацію для конкурентної боротьби;мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей.

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як «комп'ютерне піратство».Для запобігання можливих загроз, фірми повинні не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але і спробувати виявити категорії порушників і ті методи, які вони використовують.

У залежності від мотивів, мети і методів, дії порушників безпеки інформації можна розділити на чотири категорії:шукачі пригод;ідейні «хакери»;«хакери»- професіонали;ненадійні (неблагополучні) співробітники.

Шукач пригод вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись зі складнощами. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Ідейний «хакер» вибирає собі конкретні цілі (хости і ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Web-сервера абоблокування роботи ресурсу, що атакується. «Хакер»-професіонал має чіткий план дій і націлюється на визначені ресурси. Його атаки добре продумані і звичайно здійснюються в кілька етапів. Спочатку він збирає попередню інформацію. Потім він складає план атаки з урахуванням зібраних даних і підбирає (або

навіть розробляє) відповідні інструменти. Далі, провівши атаку, він одержує закриту інформацію і, нарешті, знищує всі сліди своїх дій. Ненадійний (неблагополучний) співробітник своїми діями може спричинити стільки ж проблем (буває і більше), скільки промисловий шпигун, до того ж, його присутність звичайно складніше знайти. Небезпека його несанкціонованого доступу до корпоративним даних набагато вища, ніж будь-якого іншого зловмисника.

Таким чином, інформаційна безпека є невід'ємною складовою системи економічної безпеки підприємства.Особливої уваги потребує реальне втілення запропонованих заходів щодо забезпечення інформаційної безпеки, які мають стати основою для формування та реалізації інформаційноїполітики підприємства, захисту інформації відвнутрішніх та зовнішніх загроз.

Список використаних джерел

1. Курушин В.Д. Компьютерныепреступления и информационнаябезопасность / В.Д. Курушин, В.А. Минаев. – М.: Новый юрист. –2012. – 256 с.

2. Про основні засади інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січня 2007 р. // Офіційний вісник України. – 2007. – №8. – Ст. 273.

3. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс] / Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

Пронозюк О. І.,
студент напряму підготовки6.030504 «Економіка підприємства»
економічного факультету Кам'янець-Подільського
Національного університету імені Івана Огієнка.
Науковий керівник: к.е.н., доцент Лисак В. Ю.

ПРОБЛЕМИ РОЗВИТКУ ІННОВАЦІЙ В УКРАЇНІ

Інновації є головною рушійною силою економічного зростання [1].Поняття «інновація» часто вузько трактується як «технологічна новинка». Однак його необхідно розуміти набагато ширше: «нововведення – це генерування, прийняття і впровадження нових ідей, процесів, продуктів і послуг» [2, с. 38].

Україна має свій унікальний досвід щодо впровадження інноваційної моделі економічного розвитку, який сьогодні можна охарактеризувати як досвід спроб і помилок. До 1991 року Україна мала потужний науковий потенціал європейського рівня, виділяючи на потреби науки і технологій близько 3 % ВВП - рекордний показник на ті часи (табл. 1).

Таблиця 1

Наукові кадри та кількість організацій, обсяг виконаних наукових та науково-технічних робіт в Україні з 1996 по 2012 рр.

Роки	К-сть організацій, які виконують наукові дослідження	Чис. науковців,осіб	Всього, у фактичних цінах	У тому числі				Питома вага обсягу виконаних наукових робіт у ВВП
				фундаментальні	прикладні	розробки	послуги	
			млн.грн.					%
1996	1435	160103	1111,7	140,6	321,6	606,9	42,6	1,36
2000	1490	120773	1978,4	266,6	436,7	1106,3	168,8	1,16
2005	1510	105512	4818,6	902,1	708,9	2406,9	800,7	1,09
2011	1255	84969	10349,9	2205,8	1866,7	4985,9	1291,5	0,79
2012	1208	82032	11252,7	2621,9	2057,7	5369,9	1203,2	0,8

*Дані державного комітету статистики України

Уже в 1996 році кількість працівників, задіяних у виконанні НДДКР, скоротилася вдвічі, а сукупний рівень фінансування науки впав до 1,3 % ВВП [1].

В Україні є тенденція до поступового згортання науково-технічного потенціалу. З роками зменшилась кількість організації, які виконують наукові дослідження й розробки на 16% в 2012 році в порівнянні з 1996, відчутно скоротилась чисельність науковців, а це близько 49% у 2012 в порівнянні з 1996, як результат зменшилась частка виконаних наукових і науково-технічних робіт у ВВП з 1, 35 % до 0,8 %. Загалом дані таблиці свідчать про негативну динаміку наукових кадрів, кількості організацій та обсягу виконаних наукових та науково-технічних робіт в Україні.

Бюджетні видатки на науку, починаючи від 1991 року, не перевищували 0,4 % ВВП (табл. 2), при законодавчо визначеному мінімумі в 1,7 %. [3]

Таблиця 2

Динаміка витрат держбюджету на науково-технічні роботи в Україні з 1996 по 2010 рр.

Рік	1996	2000	2005	2008	2009	2010
Витрати Держбюджету на наукові та науково-технічні роботи в Україні, % ВВП	0,46	0,36	0,42	0,41	0,37	0,34

*Дані державного комітету статистики України