– вища ланка.

Менеджери виробничих процесів користуються інформацією з перших джерел, оскільки вони особисто формують цю фактичну інформацію. Але і їм у ряді випадків потрібна для аналізу узагальнена за певний період часу інформація на рівні їхньої виробничої дільниці. Тому система об'єктивного інформування оперативно забезпечує згаданих менеджерів необхідною інформацією як в узагальненому, так і в аналітичному вигляді.

Сферою діяльності менеджерів середнього рівня є вся виробничо-господарська та інша діяльність цехів, за яку вони відповідають. Для прийняття рішення цим менеджерам необхідна узагальнена інформація.

Менеджерам виробництва вищого рівня потрібна інформація про загальний стан виробництва на кожний момент часу, кон'юнктуру ринку і т.д.

Ефективність роботи менеджера залежить як від його вміння працювати з людьми, так і від того, як він працює з інформацією.

Для виконання своїх функцій менеджерам необхідні ефективні комунікації. Комунікації – це обмін інформацією, її змістом між двома і більше людьми (працівниками). Комунікації є процесами зв'язку між працівниками, підрозділами, організаціями тощо. Комунікації супроводжують усі процеси, що відбуваються в організації.

При використанні інформаційних систем підприємство стикається з проблемою інформаційної безпеки. Інформаційна безпека полягає в збереженні конфіденційності, цілісності й доступності інформації. Конфіденційність міститься в забезпеченні доступу до інформації тільки для авторизованих користувачів, що мають право на доступ до неї, цілісність – в захисті точності й повноти інформації й методів її обробки, доступність – в забезпеченні доступності інформації й пов'язаних з нею ресурсів авторизованим користувачам за необхідності тощо.

Стандарти безпеки містять рекомендації з управління інформаційною безпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, що забезпечують безпеку в організації. Так, наприклад, стандарт ISO/IEC 17799 2005 призначений для використання будь-якою організацією, котра планує встановити систему ефективного інформаційного захисту або покращувати існуючі методи інформаційного захисту. Загальноприйняті стандарти безпеки повинні послужити основою для розробки стандартів безпеки й ефективних методів управління безпекою в конкретній організації. Крім того, вони допоможуть підтримати взаємну довіру при контактах між підприємствами і організаціями.

Література

1. Основи інформаційних систем: навч. посібник.- Вид. 2-ге, перер. І доп. / [В.Ф. Ситник, Т.А. Писаревська, Н.В. Єрьоміна, О.С. Краєва; За ред. В.Ф. Ситника]. – К.: КНЕУ, 2001. – 420 с.
2. Інформаційні системи в менеджменті: навч. посібник [Батюк А.Є., Двуліт З.П, Обельовська К.М., Огородник І.М., Фабрі Л.П]. – Львів: Нац. університет «Львівська політехніка», «Інтелект-Захід», 2004. – 520 с.
3. Кузьмін О.Є. Основи менеджменту: Підручник / О.Є. Кузьмін, О.Г. Мельник. – Львів: Нац. університет «Львівська політехніка» , «Інтелект-Захід», 2002. – 344 с.
4. Соболь С.М. Менеджмент. Навчально-методичний посібник для самостійного вивчення дисципліни / С.М. Соболь, В.М. Багацький. – К.: КНЕУ, 2002.

ІНФОРМАЦІЙНІ СИСТЕМИ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

О.І. Савченко, *магістр економічної кібернетики*
ДВНЗ «Київський національний економічний університет ім. В. Гетьмана»

Висвітлюється проблематика безпеки електронної пошти, можливість удосконалення електронної пошти для довіри до неї фахівців великих компаній

Нині розвиток інформаційних технологій продовжує стрімко прогресувати. Разом з тим зростає зацікавленість бізнесу і населення у сервісах глобальної мережі Інтернет. Бізнес-еліта зрозуміла, що не потрібно ігнорувати глобальну мережу Інтернет, оскільки за допомогою цієї мережі можна збільшувати об'єми прибутку, використовувати її для більш злагодженої роботи, залучати потенційних клієнтів, розвиватися, не дивлячись на кризу, тощо. До того ж використання мережі Інтернет не потребує великих витрат, при цьому забезпечуючи швидкий доступ до інформації в усьому світі.

Для сьогоднішнього клієнта електронні ресурси стають все більш привабливими та зручнішими, через значний зріст рівня обізнаності про них. Звісно, за таких умов зростає чисельність людей, які хочуть «поліпшити свій матеріальний стан» через необережність і несумлінність тих, хто ігнорує інформаційну безпеку.

Сьогодні електронна пошта найчастіше асоціюється з глобальною мережею Інтернет через появу численних безкоштовних серверів електронної пошти. Але не завжди електронна пошта була сервісом насамперед глобальної мережі Інтернет, раніше електронна пошта застосовувалася в локальній мережі. До речі, певні компанії досі користуються такою поштою.

Електронна пошта набула великої поширеності і серед пересічних користувачів, і серед персоналу й керівництва компаній, яким вона необхідна для злагодженої роботи. Найпопулярнішими поштовими серверами для України є ukr.net (6 334 541 поштових скриньок), gmail.com, i.ua, mail.ru (50 000 000 користувачів щомісяця), yandex.ru (9 948 100 поштових скриньок), meta.ua, rambler.ru, і кожного дня ці значення зростають.

Електронна пошта, або E-mail (від англ. *Electronic Mail*) – поширений сервіс в Інтернеті, що робить можливим обмін даними будь-якого змісту (текстовими документами, аудіо- і відеофайлами, архівами, програмами) [2].

Електронна пошта – один з найважливіших інформаційних ресурсів Інтернету, його основний засіб комунікацій в глобальній мережі [3].

Сьогодні загальноприйнятим у світі протоколом обміну електронною поштою є SMTP (від англ. *Simple Mail Transfer Protocol* – простий протокол передачі пошти). У загальноприйнятій реалізації він використовує DNS (від англ. *Domain Name System*) – службу доменної системи імен – для визначення правил пересилання.

На всіх рівнях управління корпораціями використовується електронна пошта. Однак вона дуже вразлива, оскільки не захищена: стандартні протоколи отримання і відправки пошти не використовують ніяких засобів захисту. Виходячи з цього, є ймовірність перехоплення електронної пошти під час відправки з корпорації або ж негласної змови з провайдером, який обслуговує почтові сервера цієї корпорації, і отримання копій усіх електронних повідомлень на чужу адресу.

Чому ж електронна скринька так приваблива для сторонніх осіб? У кожного свої інтереси до неї: у когось це цікавість до замовлення за гроші, у когось – до електронної бази даних клієнтів. Шахраї постійно шукають вразливості в системі електронної пошти.

Вирішенням може стати захист електронної пошти на рівні протоколів або ж використовувати методи захисту трафіку на рівні IP-пакетів. Другий варіант дозволяє більш досконало використовувати захищений канал зв'язку без прив'язки до протоколів прикладного рівня. Методи захисту можна комбінувати. Увесь процес здійснюється за допомогою стандартних засобів операційної системи (ОС) Microsoft Windows. Але слід пам'ятати про те, що клієнтська сторона є вразливою для різних шпигунських програм, які можуть перехоплювати всю інформацію користувача і приховано, непомітно відправляти її конкуренту-замовнику. Тобто при наявності шпигунської програми весь захист марний. Тому необхідно використовувати ще додаткові програмні продукти для захисту самого комп'ютера. [1]

Література

1. Сайт Википедии. – Метод доступу на 23.04.2010: <http://ru.wikipedia.org>.
2. Вікіпедія. Електронна пошта. – Метод доступу на 23.04.2010: <http://uk.wikipedia.org/wiki/Електронна_пошта>.
3. Левин М. E-mail «безопасная»: Взлом, «спам» и «хакерские» атаки на системы электронной