мою формою державної підтримки фінансового оздоровлення підприємства. Податковий механізм фінансового оздоровлення передбачає надання фінансової підтримки як на поворотній (податкові канікули, реструктуризація податкового боргу, тощо) так і на безповоротній (списання податкового боргу, надання пільг, тощо) основах. Податковий механізм в управленні фінансовим оздоровленням повинен орієнтуватися на досягнення стратегічних цілей та конкретних завдань їх реалізації, встановлення ієрархії цілей за строками досягнення і ефективності рішення проблем фінансового оздоровлення; вибір оптимального варіанта податкового регулювання діяльності кризових підприємств; поетапне досягнення цілей. Розробка оптимального податкового механізму є важливим засобом запобігання виникненню та виходу підприємств з кризового стану, який дозволить їм успішно функціонувати. На даному етапі розвитку економіки України доцільно також використовувати податкові пільги та знижки саме для стимулювання позитивних зрушень в процесах оздоровлення підприємств. Підтримка з боку держави через елементи податкового механізму процесів фінансового оздоровлення повинна орієнтується передусім на підприємства, які здатні її використати з максимальною віддачею та забезпечити свій фінансово-економічний розвиток, що в перспективі. позитивно впливатиме на формування доходної частини бюджету та загального розвитку держави.

Не дивлячись на неоднозначність і суперечливість явища банкрутства в Україні, необхідно розуміти, що банкрутство є нормальною процедурою, спрямованою на відновлення платоспроможності боржника або його ліквідації в разі неможливості подальшої діяльності. Проте наявність в Україні значної кількості збиткових підприємств унеможливлює використання повною мірою процедур банкрутства. Тому пріоритетним буде застосування щодо неплатоспроможних вітчизняних підприємств санаційних процедур перед ліквідаційними. Крім того, останні роки в Україні сформувався високоприбутковий бізнес на банкрутствах, що зумовило появу підприємств, які займаються саме цим вузькоспеціалізованим видом діяльності.

Лутература

1. Закон України «Про відновлення платоспроможності боржника або визнання його банкрутом», від 14.05.1992, N 2343-XII, внесення змін від 04.06.2009 № 1442-VI /1442-17.

2. 2. *Леонов Д. В.* Фінансова криза та український бізнес / В. Д. Леонов // Цінні папери України. — 2008. — № 42. — С. 17-20.

3. Шапурова О. О. Політика антикризового управління при загрозі банкрутства / Актуальні проблеми економіки: Науковий економічний журнал. — № 8 (86), 2009. — с. 147-153. — 270 с.

4. http:// www.sdb.gov.ua

5. http:// www.Korespondent.net.

УДК 336

ВИЗНАЧЕННЯ ЕКОНОМІЧНО ЕФЕКТИВНОГО ПІДХОДУ ДО ОРГАНІЗАЦІЇ РОБОТИ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Гриджук Г.С.

В статті розглянуто функції та програму діяльності служби інформаційної безпеки підприємства та запропоновано економічно ефективний підхід до місця та штатної чисельності працівників служби інформаційної безпеки у структурі підприємства.

The article deals wits the functions and application of information security services and proposes cost effective approach to space and staff of information security services in the structure of the enterprise.

Постановка проблеми. Світова економічна криза загострила проблему інформаційної безпеки підприємств. Разом з рівнем конкурентності середовища вона підвищила вимоги до якості та надійності не лише товарів та послуг, а й до підтримки належного рівня безпеки самих підприємств, що вступають в ділові взаємозв'язки. Своєчасне виявлення і нейтралізація загроз безпеці є першочерговим завданням всіх суб'єктів економічної діяльності. Враховуючи висококваліфікований характер ретельно організованих інформаційних атак, забезпечення безпеки підприємства на необхідному рівні можливе лише на основі науково обгрунтованої, максимально адаптованої до обстановки комплексної програми захисту інфор-

маційних ресурсів з відповідним її матеріальним та кадровим забезпеченням. Постає питання комплексного вирішення проблеми інформаційної безпеки підприємства, що вимагає створення служби безпеки, яка б проводила постійний контроль за дотриманням заходів інформаційної безпеки, інструктаж співробітників щодо використання інформаційних та технічних ресурсів підприємства, оскільки інформаційна безпека — це не низка випадкових заходів, а безперервний процес.

Аналіз останніх досліджень і публікацій. Сьогодні, коли потреба в забезпечені інформаційної безпеки підприємства є очевидною, ведуться дискусії щодо підходів до організації системи безпеки та служби, що її забезпечує. Виникають питання ієрархічної побудови, штатної чисельності служби інформаційної безпеки та її підпорядкування. Науковці [1-2] вирішують цю проблему шляхом дотримання всіх визначених вимог та побудови системи інформаційної безпеки з необмеженим бюджетом, достатньою кількістю кваліфікованих спеціалістів та технічних засобів. Практики [3-8] ж шукають ефективної реалізації проблеми інформаційної безпеки за принципом: безпека для бізнесу, а не бізнес для безпеки.

Метою статті є визначення економічно ефективного підходу до місця та штатної чисельності працівників служби інформаційної безпеки у структурі підприємства з огляду на її функції та програму діяльності.

Виклад основного матеріалу Проектувати службу безпеки необхідно одразу ж, як тільки на підприємстві з'являється інформація, що потребує посиленого захисту, втрата якої може становити реальну небезпеку благополучному розвитку підприємства, а саме: витік закритої інформації, розголошення комерційної таємниці, що тягнуть за собою фінансові та матеріальні збитки, загрозу керівництву підприємства чи його співробітникам. Робота служби інформаційної безпеки (як і всього підприємства) повинна організовуватись в суворій відповідності до законодавства держави.

Служба інформаційної безпеки підприємства повинна забезпечувати виконання функції з

— організації і координації робіт, пов'язаних із захистом інформації на підприємстві;

— дослідження технології обробки інформації з метою виявлення можливих каналів витоку та інших загроз безпеки інформації, формування моделі загроз, розробка політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

— розробки проектів нормативних та розпорядчих документів, що діють в межах підприємства, відповідно до яких повинен забезпечуватися захист інформації;

— виявлення та знешкодження загроз;

— реєстрації, збору, зберігання, обробки даних про всі події в системі, які мають відношення до безпеки інформації;

— формування у персоналу і користувачів інформації підприємства розуміння необхідності виконання вимог нормативно-правових актів, розпорядчих документів, що стосуються захисту інформації.

Реалізацію такого ряду функцій уможливлює наступна програма, яка передбачає:

1. Перевірку службою інформаційної безпеки та співбесіду з кандидатами при прийомі на роботу.

2. Навчання основам безпеки новоприйнятих працівників і сторонніх фахівців за контрактом, ознайомлення з нормативними документами з безпеки, тестування на рівень кваліфікації для роботи з інформаційними системами і одержання від них зобов'язання дотримуватись нормативів організації (в тому числі і з безпеки).

3. Співбесіду представника служби безпеки з працівником, що звільняється. Звільнення працівника відразу відображається в інформаційних системах (блокування та видалення облікових записів, вилучення карток доступу і т.д.).

4. Проведення періодичних семінарів та навчання з інформаційної безпеки для співробітників організації.

5. Проведення аналізу моральної та психологічної ситуації в організації, обліку порушень безпеки конкретними співробітниками. При цьому заохочується тісний інформаційний контакт користувачів зі службою безпеки, вибірково або постійно аналізується електронна пошта співробітників з відповідним нормативним оформленням процедури.

6. Регулярне проведення авторизованого моніторингу активності користувачів на робочій станції. Всі дані, об'єкти та інформаційні системи класифікуються. Суб'єкти розподіляються за ролями.

7. Побудову та функціонування надійної структури та механізм доступу суб'єктів до об'єктів з урахуванням найменших привілеїв і поділу обов'язків. Кожен новий об'єкт вчасно класифікується і встановлюється в загальну схему інформаційного простору.

8. Забезпечення нормативного простору. Для всіх інформаційних систем існують політики, для функціональних обов'язків користувачів — правила, процедури та методики. Зміни в роботі організації та співробітників адекватно відображаються у відповідних документах.

9. Контроль служби інформаційної безпеки за способами аутентифікації користувачів, тобто проводиться періодичний аналіз відсутності слабких паролів, фактів передачі паролів іншим особам, залишення токенів без нагляду і т.п. Ідентифікація користувачів стандартизована, є чітка таблиця відповідності користувач — мережеві адреси, дозволені для роботи даного користувача.

10. Обмеження зовнішнього віддаленого доступу в інформаційну мережу підприємства (вихід у зовнішню інформаційний простір) єдиним центральним шлюзом, наявність резервного каналу зв'язку, неактивного в штатному режимі.

11. Захист каналів міжмережевими екранами, які надійно функціонують, коректно налаштовані і регулярно піддаються перевірці службою інформаційної безпеки. Всі модеми та інші пристрої віддаленого доступу враховуються і також зводяться до зазначеної єдиної точки входу/виходу. Зовні по відношенню до точки входу встановлюється агент мережевої системи виявлення атак (СВА), який присутній на кожному сегменті в мережі організації. Проведення періодичного аналізу мережевої активності засобами мережевого моніторингу та реєстраційних журналів (які налаштовані на фіксацію всіх подій), у тому числі особисто уповноваженим персоналом.

12. Ведення реєстраційних журналів всіх інформаційних систем, регулярну автоматизовану обробку цих журналів, а також періодичний вибірковий ручний їх аналіз на предмет виявлення підозрілих або злочинних подій. Інтеграцію системи аналізу інформаційної активності з системою фізичного доступу співробітників в будівлю і до робочих місць. Зберігання поряд з журналами резервних копій та архівів бізнес-даних.

13. Встановлення на кожному комп'ютері антивірусного пакету, крім того на поштовому сервері, міжмережевому екрані та інших ключових вузлах. Режим роботи антивіруса — autoprotect. Антивірусні бази оновлюються щодня, а також при надходженні інформації про новий вірус.

14. Ведення суворого обліку руху апаратного забезпечення та його складових, а також апаратної та програмної конфігурації кожного об'єкта або системи. При зміні конфігурації негайно проводиться збереження відповідних установок. Ведеться регулярний моніторинг продуктивності роботи апаратного забезпечення, операційних систем, інформаційної системи в цілому.

15. Вивчення повідомлень про нові атаки, віруси, вразливі місця тощо, нові рішення і механізми з безпеки. Проведення аналітичної роботи з визначення тенденцій розвитку атак, появи вразливих місць, нових продуктів на ринку безпеки, нових технологій.

16. Криптографічний захист всіх каналів обміну даними в інформаційній мережі, локальній мережі, організованих віртуальних мережах. Будь-який обмін даними реєструється в електронних журналах і забезпечений засобом контролю цілісності. Забезпечено контроль цілісності даних, системних файлів і т.п. на серверах і робочих станціях. Обмін даними між користувачами здійснюється з використанням електронного цифрового підпису. Організовано надійне управління криптографічними ключами.

17. Забезпечення контролю вхідної та вихідної інформації на зовнішніх носіях. Встановлення надійного захисту шлюзів обміну інформацією з зовнішніми інформаційними системами Регулярне проведення процедури тестування всієї мережі або окремих систем на надійність.

18. Роботу в службі інформаційної безпеки команди програмістів зі створення власних програм або утиліт для аналізу захищеності або, навпаки, для захисту об'єктів і систем.

19. Забезпечення резервного копіювання даних, збереження архівів і резервних копій, швидкої заміни мережевих пристроїв.

20. Забезпечення безперервної роботи інформаційної системи: безперебійне електроживлення (і контроль за його роботою), наявність функціональними дублерів ключових працівників організації, регулярно оновлюваний аварійний план.

21. Участь служби інформаційної безпеки у всіх проектах організації (в тому числі і в розробці програмного забезпечення) з правом внесення серйозних змін і заборон у рамках своїх функцій. Служба має повноваження для прийняття та реалізації рішень, пов'язаних з інформаційною безпекою.

22. Встановлення системи відволікання уваги зловмисника (honeypot), формування власної команди реагування на інциденти, встановлення зв'язку з аналогічними командами інших організацій, зовнішніми експертами, силовими структурами.

23. Забезпечення узгодженого управління всіма автоматизованими засобами інформаційної безпеки.

Для виконання всіх перелічених процедур в службі інформаційної безпеки повинно бути задіяно кілька десятків, а той сотень спеціалістів. Звичайно для великих компаній, що турбуються про якісний рівень безпеки і постійно працюють над власним іміджем та зростанням інформаційного потенціалу така програма ІБ і багаторівнева структура служби ІБ (рис.1) будуть виправданими.

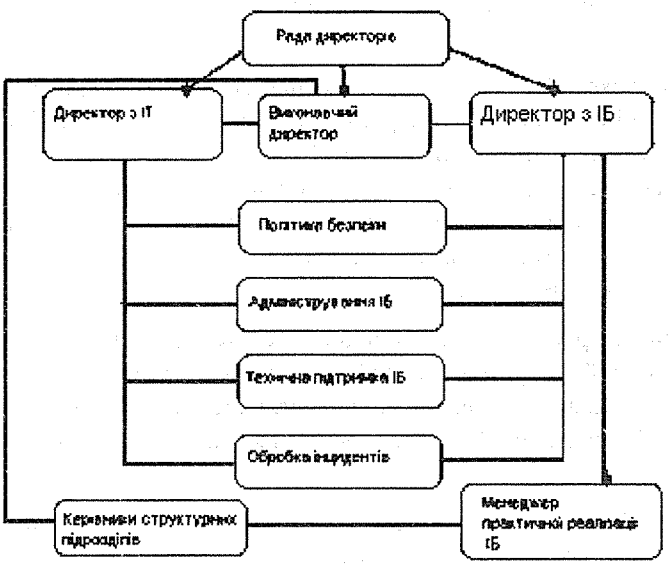

Рис. 1. Структура служби інформаційної безпеки підприємства

Проте на практиці, як правило, не вдається реалізувати цю ідеальну програму повністю. Не всі підприємства спроможні нести витрати із забезпечення такої повномасштабної системи безпеки, тому необхідно економічно обґрунтувати її склад, структуру, чисельність, підпорядкування та взаємозв'язки.

Ми пропонуємо кілька підходів до вирішення даної проблеми. Малі підприємства за якісними послугами безпеки «за розумні гроші» можуть звернутись до аутсорсингових компаній, які пропонують цілий ряд найрізноманітніших ІТ-послуг та програм захисту, а також комплекс економічно обґрунтованих рішень проблем безпеки для підприємств різних галузей народного господарства. Підвищити рівень власної безпеки підприємство може шляхом поєднання послуг аутсорсингових компаній з власним контролем. Проте в кожному з цих двох випадків підприємства залишаються залежними від компанії, яка їх обслуговує, що віддаляє їх показник безпеки від абсолютного рівня.

Більші підприємства, що пройшли період становлення і зацікавлені в створенні позитивної репутації та підвищенні економічних показників своєї діяльності шляхом активного впровадження новітніх технологій та методик, виконання завдань безпеки покладають на менеджерів ІТ-підрозділу. Теоретично таке рішення має право на існування, оскільки ІТ-спеціалісти є хорошими фахівцями в питаннях управління апаратно-програмного комплексу інформаційної безпеки. Проте у вирішенні проблем організаційного та правового характеру вони можуть стикнутися з цілим рядом труднощів. Тому ризик погіршення якості виконання прямих обов'язків ІТ-менеджерів через реалізацію додаткових функцій безпеки не завжди компенсуватиметься забезпеченням належного рівня інформаційної безпеки. Виникають проблеми також з питанням підпорядкування.

Оптимальним підходом до результативного та ефективного вирішення проблем інформаційної безпеки є створення відповідного самостійного підрозділу, підпорядкованого безпосередньо першій особі в організації. Спроби вирішити проблему іншим способом дозволяють, у кращому разі, домогтися успіху частково. Неважко підрахувати, що утримання служби інформаційної безпеки з трьох осіб (мінімальний склад

відділу інформаційної безпеки — начальник, аналітик і адміністратор ІБ) обійдеться компанії набагато дешевше можливих збитків. Даний відділ не буде приносити явного прибутку, проте його призначення — зменшення збитків від можливих загроз. А їх діапазон залежатиме від сфери діяльності підприємства та рівня конфіденційності інформації, що в ньому функціонує.

Висновки з даного дослідження та перспективи подальших досліджень у даному напрямку

Проведений аналіз запропонованих підходів до місця та штатної чисельності працівників служби безпеки у структурі підприємства дає підстави зробити висновки про їх залежність від архітектури підприємства, стратегії його розвитку, технологій, що впроваджені, процесів, що відбуваються всередині підприємства та за його межами, а також від людського фактору, який є визначальним для культури підприємства та його управління. Чисельність і склад служби інформаційної безпеки повинні бути достатніми для виконання всіх завдань безпеки і захисту інформації. Економічно виправданим з точки зору результативності та ефективності буде створення на підприємстві служби інформаційної безпеки, як самостійного підрозділу, що підпорядковується безпосередньо керівнику підприємства та активно співпрацює з IT-службою, утворюючи стійку «трикутну» структуру — «аудит — служба інформаційної безпеки — IT-служба». Подальші дослідження планується проводити в напрямку визначення границь управління інформаційною безпекою та меж її відповідальності, щоби служба безпеки не перетворювалася на нікому не підвладного, контролюючого всіх монстра. Запорукою успіху є повноцінна взаємодія служби інформаційної безпеки з усіма співробітниками підприємства, оскільки реально його інформаційною безпекою займаються всіСлужба безпеки — тільки контролює, навчає і управляє зусиллями користувачів інформації.

Література

1. http://web-protect.net.
2. Лукацкий А. В. Информационная безопасность. Как обосновать. Компьютер Пресс, 2000, №11
3. Владимир Безмалый. Создание отдела информационной безопасности// Директор ИС. http://www.osp.ru.
4. http://www.microfinance.uz.
5. http://all-ib.ru.
6. http://www.sec4all.net.
7. Беркман Э. Как подобрать персонал для обеспечения безопасности// ДИС, 2002, № 12.
8. Безмалый В. Ф. Безмалая Е. В. Создание отдела информационной безопасности, или Строим забор своими руками. http://www.diwaxx.ru/hak/zabor.php.

УДК 330.145

ОСОБЛИВОСТІ КРУГООБІГУ КАПІТАЛУ ПАСАЖИРСЬКИХ АТП І НЕОБХІДНІСТЬ КРЕДИТУ

Даценко М.В.

В процесі кругообігу капіталу відбувається зміна його форм: грошова форма переходить у виробничу, виробнича форма змінюється товарною і на третій стадії відбувається повернення до початкової грошової форми. Знаходження капіталу одночасно своїми частинами в усіх трьох стадіях і в усіх трьох формах забезпечує безперервність виробничого процесу, а, відповідно, і споживання. При затримці руху капіталу на одній зі стадій порушується нормальний хід кругообігу.

In the process of circulation of capital it's forms are changing: cash goes into production, commodity production is changing shape, and the third stage there is a return to the initial cash. Capital location in its parts simultaneously in all three stages and forms ensures continuity of production, and, respectively, consumption. In case of delay of the movement of capital in one of the phases of the cycle the normal course is interrupted.

В економічній теорії і підприємницькій практиці, мабуть що, нема поняття, яке б використовувалося так часто і одночасно так неоднозначно як «капітал». Неоднозначність цього терміну особливо очевидна останнім часом. В економічній літературі існують точки зору прихильників різних концепцій по даному дискусійному питанню, що дозволяє проаналізувати основні визначення капіталу. Початково поняття