6. Зайченко Ю.П. Дослідження операцій : навч. посібн. [для студ. ВНЗ] / Ю.П. Зайченко. – Вид. 4-те, [перероб. та доп.]. – К. : ЗАТ "ВІПОЛ", 2000. – 687 с.

7. Калихман И.Л. Динамическое программирование в примерах и задачах : учебн. пособ. / И.Л. Калихман, М.А. Войтенко. – М. : Изд-во "Высш. шк.", 1979. – 125 с.

8. Квик М.Я. Задача про оптимальне розміщення підприємств та метод її розв'язування / М.Я. Квик, Г.Г. Цегелик // Вісник ЛДФА. – Сер.: Економічні науки. – 2009. – № 17. – С. 244-253.

9. Квик М. Відшукання найкоротших шляхів у транспортній мережі методом динамічного програмування / М. Квик, Г. Цегелик, Я. Романчук // Вісник Львівського університету. – Сер.: Економічна. – 2010. – Вип. 43. – С. 25-31.

10. Цегелик Г.Г. Використання математичних методів і моделей для дослідження економічних процесів / Г.Г. Цегелик // Сучасні інформаційні технології в економіці, менеджменті та освіті : матер. Всеукр. наук.-практ. конф. – Львів. – 2010. – С. 15-22.

11. Петлін І.В. Оптимізація розподілу інвестиційних коштів як фактор розвитку малого підприємництва у сфері сільського зеленого туризму / І.В. Петлін, Г.Г. Цегелик // Вісник Хмельницького національного університету. – Хмельницький : Вид-во ХНУ. – 2012. – № 1(184). – С. 93-99.

Петлин И.В., Цэгэлык Г.Г. **Использование метода динамического программирования для повышения эффективности инвестиционной деятельности в сфере сельского зеленого туризма**

Проанализированы препятствия на пути активизации инвестиционной деятельности в туристической отрасли вообще и в сельском зеленом туризме в частности. Для повышения эффективности инвестиционной деятельности в сфере сельского зеленого туризма предлагается использовать метод динамического программирования для распределения инвестиционных средств среди сельских регионов, который обеспечивает максимальную прибыль субъектам малого предпринимательства в сфере этой. Приведен алгоритм оптимального распределения инвестиций в общем виде, работа которого проиллюстрирована на конкретном примере.

Ключевые слова: туризм, сельский зеленый туризм, инвестиции, метод динамического программирования.

Petlin I.V., Tsegelik G.G. **Dynamic programming method for increase the efficiency of investment activity in the rural green tourism**

The obstacles of active investment activity in tourist industry and rural green tourism are analysed. A dynamic programming is needful for increase the efficiency of investment activity in the rural green tourism and for distribution the investment money among rural regions. It will provide maximal income to small business entities. The algorithm of optimal distribution the investments is determined. It is produced in concrete example.

Keywords: tourism, rural green tourism, investments, dynamic programming method.

УДК 004.056:061.68

Студ. К.В. Мілян, магістрант;
проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ПРОМИСЛОВОЇ КОМПАНІЇ

Розглянуто особливості організації інформаційної безпеки (ІБ) корпоративної мережі промислової компанії, яка дає змогу їхнім керівникам впевнитися у тому, що конфіденційна інформація не потрапить до зловмисників чи до рук компаній-конкурентів і не завдасть шкоди самій компанії. З'ясовано, що реалії сучасного бізнесу – це доступ відповідних працівників компанії до її інформаційних ресурсів з будь-якої точки місця перебування, використання ними особистих мобільних пристроїв для вільного переміщення конфіденційних даних усередині корпоративної мережі та за її межами, що призводить до серйозних ризиків забезпечення безпеки господарської

діяльності компанії. Тому керівникам служб ІБ корпоративних мереж компаній доводиться враховувати багато особливостей захисту інформації, а також знати, за допомогою яких засобів може забезпечуватися реалізація тих чи інших завдань ІБ.

Ключові слова: інформаційні загрози, інформаційна безпека, інформаційні технології, джерела загроз, промислова компанія.

Вступ. Темпи сучасного інформаційного розвитку такі, що значущість і стабільність бізнесу тої чи іншої компаній все менше залежать від її матеріальних активів [4]. Закріпившись на ринку товаровиробників і продовжуючи набирати темпи товарообігу, сучасними активами будь-якої компанії можна вважати наявну інформацію про споживачів своєї продукції та своїх конкурентів. Іншими словами, практично неможливо уявити призначення тої чи іншої промислової компанії, яка не володіє достеменною інформацією про свій ринок товарообігу [7]. Це означає, що для компанії, яка націлена на довготермінове і серйозне існування, особливо важливо, щоб власна інформаційна безпека (ІБ) була організована на найвищому рівні [10].

Джерелами інформаційних активів можуть слугувати [12]: засновники бізнесу, посадові особи та співробітники компанії, клієнти компанії та постачальники сировини чи напівфабрикатів, державні та приватні замовлення, результати різних маркетингових досліджень, власна комерційна діяльність та компаній-конкурентів, схеми фінансових платежів тощо. Така інформація є ключовим елементом у діяльності кожного серйозного керівника та його заступників, а також працівників служби ІБ, які мають оберігати її від зазіхань конкурентної розвідки [14], а також витоку через своїх працівників-інсайдерів[1].

Тому основною *метою роботи* є аналіз особливостей організації інформаційної безпеки корпоративної мережі промислової компанії, яка дасть змогу їхнім керівникам бути впевненим у тому, що конфіденційна інформація не потрапить до зловмисникові чи компаній-конкурентів і не завдасть шкоди самій компанії. Основні завдання роботи полягають у: виявленні особливостей організації служби ІБ промислової компанії; розгляді наявних її політик ІБ; наданні практичних рекомендацій щодо організації корпоративної ІБ промислової компанії.

1. Організація служби ІБ промислової компанії. При організації інформаційного захисту навіть невеликої компанії не варто застосовувати "фрагментарну" безпеку її мережевої інфраструктури [9]. Водночас, немає сенсу вибудовувати монументальний між мережевий екран, якщо співробітники, не докладаючи особливих зусиль, можуть винести інформацію на компакт-диску або флеш-памяті, цим самим допускаючи витік даних зсередини компанії [11]. Може тому і найбільш ефективними вважаються тільки комплексні заходи – від грамотно побудованої мережевої інфраструктури до радикального адміністративного менеджменту у сфері захисту інформації [5, 6].

Мережева безпека – складова частина загальної системи ІБ компанії, яка вирішує проблеми захищеності її інформаційних систем на рівні мереже-

[1] Інса́йдер (англ. insider) – особа (юридична або фізична), яка має доступ до конфіденційної інформації про справи компанії завдяки своєму службовому становищу, участі у формуванні капіталу компанії, родинним зв'язкам і має можливість його використовувати у власних інтересах.

вої інфраструктури [12]. Оскільки мережева безпека є однією з основних складових комплексної системи захисту інформації, то її організацією та забезпеченням має займатися компетентний фахівець – системний адміністратор [3].

Вважатимемо, що мережа надійно захищена від вторгнень: нічого не пройде повз увагу системного адміністратора, підозріла пошта відправляється "куди треба", серверні антивіруси щодня оновлюються та "просівають" весь трафік внутрішніх і зовнішніх розмов за допомогою IP-телефонії чи Skype. Хоча тут би варто задуматися – кому з конкурентної розвідки є цікавим інформаційний вміст локальної мережі навіть крупної компанії? Загалом, всіх охочих потрапити туди, куди їх не запрошують, можна розділити на дві категорії [8]: або конкуренти, або серйозні мережеві хакери. Причому останнім вміст локальної мережі може бути зовсім ні до чого, у них зовсім інші цілі.

Припустимо, компанія успішно торгує комп'ютерною технікою. Місячні товарообіги не завжди навіть мільйонні, але справа йде до зростання товарообігу. Є і постійне під'єднання до мережі Інтернет, присутній VoIP-зв'язок і виділений сервер під локальну мережу. Розумному хакеру зовсім не потрібна інформація про такий бізнес, але йому потрібна територія для нападу, наприклад, на бухгалтерську звітність чи схему фінансових платежів [14]. В цьому випадку використовувати для атаки свій особистий комп'ютер небезпечно, позаяк навіть професійний хакер може або помилитися, або залишити непомітний слід в мережі, за яким його врешті-решт виявлять [6]. Тому хакер здебільшого вибирає тимчасовий "майданчик", тобто зламується сервер будь-якої опосередкованої фірми, наприклад, з ремонту офісної техніки, потім бере його управління "на себе", і вже від імені цього сервера можна відносно спокійно заходити у бухгалтерську мережу промислової компанії, якщо в тій, зрозуміло, не будуть вчасно виявлені входження [11]. У разі виявлення атаки всі претензії пред'являються до опосередкованої фірми, яка знати нічого не знає про них, але проблему все-таки отримує і то на кримінальному рівні, а довести свою не причетність до атак – практично неможливо.

Викладене вище в черговий раз свідчить тільки про те, що безпека мережевих ресурсів необхідна завжди і в повному обсязі – як промисловій компанії, так і в будь-якій опосередкованій фірмі, які мають вихід в мережу Інтернет [3, 5, 6].

Дещо інші цілі переслідують компанії-конкуренти [14] – у них якраз є прямий інтерес ознайомитися з внутрішніми документами промислової компанії, обсягами продажів і постачання сировини чи матеріалів, майбутніми маркетинговими акціями та іншою корисною для них інформацією. Але й тут, у разі надійного захисту мережі, їм залишається або піти ні з чим, або виявити чудеса класичного шпигунства, що, зазвичай, зводиться до безпосередньої взаємодії зі співробітниками промислової компанії [10].

Так чи інакше, при правильному підході ІБ корпоративної мережі значною мірою залежить від фахових дій системного адміністратора. Йому під силу встановити потрібну програму чи видалити зайву, відкрити порт у між мережеві екрани і ще багато чого, що потенційно може підтримати чи порушити інформаційну безпеку компанії. У зв'язку з цим часто керівники

крупних компаній воліють тримати в штаті декількох осіб, які займаються такою роботою, – проконтролювати сисадміна здатний тільки інший сисадмін, але більш кваліфікований від попереднього [3].

Також не варто забувати і про проблему утилізації старого комп'ютерного обладнання [14]. Дані з електронних носіїв старих ПК копіюються на нові, але як і раніше залишаються доступними на жорстких дисках. Це стосується не тільки жорстких дисків, але й компакт-дисків, флеш-пам'яті і т. д. Якщо є підозра, що на цих носіях могла зберегтися інформація, найнадійніший шлях – спочатку фізично їх пошкодити, а вже потім утилізувати.

2. Політика ІБ промислової компанії. Політика ІБ будь-якої організації[1] – набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації та спрямовані на досягнення і підтримку стану її ІБ [12]. Політики ІБ знаходиться в основі організаційних заходів захисту інформації. Від їх ефективності найбільшою мірою залежить успішність будь-яких заходів щодо забезпечення ІБ. Часто доводиться стикатися з неоднозначністю розуміння терміну "політика інформаційної безпеки". У сучасній практиці забезпечення ІБ термін "політика ІБ" може вживатися як у широкому, так і у вузькому сенсі слова. У широкому сенсі, політика ІБ визначається як система документованих управлінських рішень з забезпечення ІБ організації. У вузькому значенні під політикою ІБ зазвичай розуміють локальний нормативний документ, який визначає вимоги безпеки, систему заходів або порядок дій, а також відповідальність співробітників організації та механізми контролю для певної області забезпечення ІБ. Прикладами таких документів можуть слугувати "Політика керування паролями", "Політика управління доступом до ресурсів корпоративної мережі","Політика забезпечення ІБ при взаємодії з мережею Інтернет" і т.п. Використання декількох спеціалізованих нормативних документів звичайно є більш привабливим створення "Загального керівництва щодо забезпечення ІБ організації". Наприклад, в компанії Cisco Systems, Inc. стараються, щоб розмір політики ІБ не перевищував 2-ох сторінок. У рідкісних випадках розмір політики ІБ може сягає 4-5 сторінок.

Як приклад корпоративної політики ІБ розглянемо комп'ютерну компанію "СофтСервіс", у якій достатньо точно і чітко регламентуються всі моменти використання мережевого обладнання та програмного забезпечення. Для розуміння її сутності та призначення наведемо деякі витяги з цього нормативного документа [4].

Мета політики ІБ полягає в тому, щоби гарантувати використання за призначенням комп'ютерної техніки і телекомунікаційних ресурсів Компанії її співробітниками, незалежними підрядниками та іншими користувачами. Всі користувачі корпоративної мережі мають використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись норм етики і чинного законодавства.

[1] Политика информационной безопасности организации. [Електронний ресурс]. – Доступний з http://www.data ved.ru/2009/03/blog-post_30.html

Політика ІБ, її правила і умови стосуються всіх користувачів комп'ютерних і телекомунікаційних ресурсів і служб Компанії, де б ці користувачі не знаходилися. Порушення цієї політики тягне за собою дисциплінарні стягнення, аж до звільнення співробітника і/або притягнення його до кримінальної відповідальності. Політика ІБ може періодично змінюватись і переглядатися в міру потреби.

Керівництво Компанії має право, але не зобов'язане перевіряти будь-який або всі аспекти інформаційної системи, яка містить електронну пошту, з метою гарантувати дотримання політики ІБ. Комп'ютери та доступи до інформаційних ресурсів надаються співробітникам Компанії з метою допомогти їм більш ефективно виконувати свою роботу.

Комп'ютерна і телекомунікаційна системи належать Компанії і можуть використовуватися тільки в робочих цілях. Співробітники Компанії не повинні розраховувати на конфіденційність інформації, яку вони створюють, посилають або отримують за допомогою комп'ютерів і телекомунікаційних ресурсів, які належать Компанії. Користувачі мають дотримувати умови всіх програмних ліцензій, авторське право і закони, що регулюють правовідносини у сфері інтелектуальної власності.

Користувачам комп'ютерів слід керуватися перерахованими нижче заходами щодо всіх комп'ютерних і телекомунікаційних ресурсів і служб Компанії, які містять таке обладнання: хост-комп'ютери, сервери файлів, робочі станції, автономні комп'ютери, мобільні комп'ютери, програмне забезпечення, а також внутрішні та зовнішні мережі (мережа Інтернет, комерційні інтерактивні служби і системи електронної пошти), до яких прямо або опосередковано звертаються комп'ютерні пристрої Компанії.

Невірні, нав'язливі, непристойні, наклепницькі, образливі, загрозливі або протизаконні матеріали забороняється пересилати електронною поштою або за допомогою інших засобів електронного зв'язку, а також відображати і зберігати їх на комп'ютерах Компанії. Користувачі, які помітили або отримали подібні матеріали, повинні негайно повідомити про цей інцидент своєму керівникові.

Все, що створене на комп'ютері Компанії, у т.ч. повідомлення електронної пошти та інші електронні документи, може бути проаналізовано керівництвом Компанії. Користувачі не мають права пересилати електронною поштою будь-які документи іншим особам і організаціям без дозволу відправника. Електронна пошта від юриста Компанії або адвоката, який представляє її інтереси, має містити в колонтитулі кожної сторінки повідомлення: "Захищено адвокатським правом/без дозволу не пересилати".

Користувачам не дозволяється встановлювати на комп'ютерах і в мережі Компанії власне програмне забезпечення без дозволу системного адміністратора. Користувачам забороняється змінювати і копіювати файли, що належать іншим користувачам, без дозволу власників файлів.

Забороняється використання без попереднього письмового дозволу комп'ютерних і телекомунікаційних ресурсів і служб Компанії для передачі або зберігання комерційних або особистих оголошень, клопотань, рекламних

матеріалів, а також руйнівних програм, політичних матеріалів і будь-якої іншої інформації, на роботу з якою у користувача немає повноважень або призначеного для особистого використання.

Користувач несе відповідальність за збереження своїх паролів для входу в систему. Забороняється роздруковувати, зберігати в мережі або передавати іншим особам індивідуальні паролі. Користувачі несуть персональну відповідальність за всі транзакції, які будь хто зробить за допомогою їхнього пароля. Можливість входу в інші комп'ютерні системи через мережу Компанії не дає користувачам права на під'єднання до цих систем і використання їх без спеціального дозволу операторів цих систем.

Прийняття політики ІБ будь-якої компанії та отримання підпису від кожного співробітника – кожен працівник зобов'язаний ознайомитися з політикою ІБ і підписатися під нею. Фактично, в нашому українському менталітеті тільки це змушує співробітників компанії уважно прочитати і вникнути в зміст документа. А у випадку його порушення – тільки це дає законне юридичне право на відповідне стягнення з співробітника.

Отже, політика ІБ промислової компанії має містити такі рішення та заходи щодо її забезпечення[1]:

- проведення аудиту ІБ та оцінювання захищеності інформаційних ресурсів компанії, підготовка її інформаційних систем для досягнення відповідності чинних вимог щодо забезпечення ІБ;
- організація комплексної системи захисту інформації, яка знаходиться в інформаційно-управлінській системі виробничо-господарської діяльності компанії, в яку внесено:
  1) комплексний захист від несанкціонованих доступів: управління доступом; реєстрація та облік подій ІБ; забезпечення контролю за цілісності та доступності інформаційних ресурсів; надійний криптографічний захист інформації;
  2) забезпечення ІБ між мережевої взаємодії: проведення між мережевого екранування та сегментації доступу до мереж; створення віртуальних приватних мереж; пошук і запобігання вторгнень та ін.;
  3) безпечний віддалений доступ до наявних корпоративних інформаційних ресурсів, в т.ч. конкретні мережі та мережі загального доступу;
  4) професійний контроль над використанням інформаційних ресурсів;
- захист інформаційно-управлінських систем спільно з:
  1) управлінням доступом на прикладному рівні, комплексним розробленням і реалізацією концепції повноважень користувачів;
  2) налаштуванням аудиту подій ІБ із під'єднанням до централізованих систем контролю над інцидентами;
  3) професійним захистом (безпечним налаштуванням) загальносистемного і спеціалізованого програмного забезпечення;
  4) захистом від несанкціонованого доступу, розмежуванням доступу;
- повне налаштування систем захисту інформації в ІС, які призначені для надійного оброблення персональних даних;
- налаштування систем контролю та захисту інформації в АСУ ТП;
- налаштування системи управління ідентифікаційними даними, централізованого управління доступом і забезпечення аутентифікації;

[1] Политика информационной безопасности компании. [Електронний ресурс]. – Доступний з http://www.security policy.ru/index.php/Политика_информационной_безопасности_компании

- оперативна доставка і супровід засобів комп'ютерної техніки.

Отже, відповідальність за дотримання політики ІБ компанії несе кожен її співробітник, при цьому першочерговим завданням є забезпечення безпеки всіх активів компанії. Це означає, що інформація повинна бути захищена не менш надійно, ніж будь-який інший основний актив компанії. Головні цілі компанії не можуть бути досягнуті без своєчасного і повного забезпечення співробітників інформацією, необхідною їм для виконання своїх службових обов'язків.

3. Організація корпоративної ІБ промислової компанії. Сьогодні все більш значущою стає проблема забезпечення внутрішньої ІБ в організаціях і компаніях [11]. Якщо раніше основним напрямком в області захисту інформації були зовнішні загрози і атаки, то на сьогодні більше 70 % витоків інформації відбувається завдяки внутрішнім загрозам ІБ [9]:

- несанкціонований витік конфіденційної інформації;
- захист електронної корпоративної пошти від спаму та вірусів;
- захист, контроль і оптимізація веб-трафіку;
- контроль доступу до корпоративної мережі;
- контроль і запис дій адміністраторів на серверах;
- моніторинг активності користувачів і їхніх дій.

Проаналізуємо кожну з цих загроз ІБ більш детально.

1) Проблема захисту інформації від її витоків стає все більш актуальною, беручи до уваги такі тенденції розвитку ІТ-сфери: зростання мобільності бізнесу та наявність внутрішніх інсайдерів [10].

Зростання мобільності бізнесу простежується у таких його проявах:

- ноутбуки поступово витісняють настільні комп'ютери (за попередніми прогнозами, до кінця 2013 року вони будуть займати близько 80 % всіх комп'ютерів);
- ємність знімних носіїв зростає, в той час, як їх вартість – зменшується;
- стандартний жорсткий дисковий накопичувач для ноутбука >500 GB;
- 8GB USB флеш-накопичувач коштує менше 15$;
- збільшення кількості витоків інформації внаслідок більшої мобільності даних;
- користувачі схильні зберігати все підряд, в т.ч. і те, що не стосується роботи;
- мобільність підвищує ризик витоку даних.

Як рекомендації що уникнення цього виду загроз доцільно використовувати шифрування інформації перед її зберіганням за допомогою різних засобів криптографічного захисту, наприклад, PGP[1], StrongDisk[2], E-NIGMA[3] і т.п. Шифрування окремих файлів і папок або повне шифрування диска із застосуванням алгоритму Advanced Encryption Standard (AES) забезпечує захист даних у випадку втрати або крадіжки пристрою. Шифрування також може застосовуватися для захисту периферійних пристроїв, знімних дисків, окремих файлів і папок. Технологія працює непомітно для кінцевих користувачів і не знижує продуктивність роботи системи.

Інший бік внутрішніх загроз – інсайдери[1]. У зв'язку з поширеністю великої кількості мініатюрних накопичувачів даних все більшу загрозу для промислової компанії приймають інсайдери – особи, що мають безпосередній або відносний доступ до її конфіденційної інформації. Володіючи легальним доступом до системи та інформації, інсайдери можуть зробити спроби її передачі третім особам, або ж використовувати цю інформацію у власних інтересах, але не в інтересах компанії. Вирішення проблеми інсайдера – впровадження системи класу Data Leak Protection[2], тобто системи контролю витоків інформації. Система проводить моніторинг та контроль за всією інформацією, яка виходить за межі периметра об'єкта ІБ, устаткування та комп'ютерів корпоративної мережі промислової компанії. З програмних рішень цього класу варто згадати таких виробників, як Lumension[3], Symantec[4] і SmartLine.

Наприклад, компанія Lumension, Inc (США) заснована у вересні 2007 року декількома компаніями внаслідок злиття трьох компаній – американської компанії PatchLink Inc, провідного розробника рішень з управління уразливими місцями і оновленнями, люксембурзької компанії SecureWave, виробника рішень для захисту кінцевої точки, і компанії Stat, творця багатофункціонального сканера для внутрішніх служб США. Сьогодні компанія Lumension Security – лідер світового ринку систем управління ІБ. Компанія пропонує уніфіковані проактивні рішення для забезпечення ІБ і гнучкого контролю всіх робочих станцій і серверів корпоративної мережі, її пристроїв і додатків. Превентивні ІТ-технології від Lumension покликані запобігти загрозам, а не боротися з їхніми наслідками, підвищити ефективність і продуктивність роботи всіх корпоративних систем, уникнути таких загроз, як крадіжка або витік інформації, шкідливе і шпигунське ПЗ, загрози нульового дня, небажане і неліцензійне ПЗ та ін. Сьогодні кількість клієнтів компанії Lumension Security перевищує 5100, це більше 14 мільйонів ліцензій в усьому світу.

[1] PGP (Pretty Good Privacy) – криптографічний додаток для забезпечення захисту та аутентифікації даних. Його використання забезпечує впевненість в тому, що ніхто не зможе прочитати або змінити інформацію. Захист гарантує, що тільки одержувач інформації зможе скористатися нею (див. www.pgpi.org).

[2] StrongDisk Pro – універсальний засіб для захисту конфіденційної інформації на персональних комп'ютерах, ноутбуках і змінних носіях. Перша версія системи з'явилася в 2000 році. Всі системи оснащені надійними апаратними засобами і базуються на найнадійніших і перевірених алгоритмах кодування з довжиною ключа до 448 біт.

[3] E-NIGMA – це платна система віддаленого зберігання конфіденційної інформації. Завдяки використанню криптографії з відкритим ключем, призначені для користувача дані на серверах компанії зберігаються в зашифрованому вигляді. Система розроблена російською компанією "Тенденція" в 2006 році.

[1] Інса́йдер (англ. insider) – особа (юридична або фізична), яка має доступ до конфіденційної інформації про справи компанії завдяки своєму службовому становищу, участі у формуванні капіталу компанії, родинним зв'язкам і має можливість його використовувати у власних інтересах.

[2] Запобігання витоків (англ. Data Loss Prevention, DLP) – технології запобігання витоків конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витокам. DLP-системи будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи, і передача повідомлення (пакету, потоку, сесії) блокується.

[3] HeadTechnology. [Електронний ресурс]. – Доступний з http://www.headtechnology.com.ua/ru/products/?sup=6

[4] Компанія Symantec є світовим лідером у виробництві програмного забезпечення, додатків та сервісів для окремих користувачів, представників малого та середнього бізнесу, та великих корпорацій і характеризується надійністю, доступністю та сумісністю. Компанія Symantec добре відома за такими програмними продуктами як антивірус та системні утиліти, знаними під брендом Norton. До них належать Norton Commander, Norton AntiVirus, Norton Internet Security, Norton Personal Firewall, Norton AntiSpam, Norton SystemWorks, Norton GoBack, Norton Ghost, Norton 360. [Електронний ресурс]. – Доступний з http://www.symantec-antivirus.com.ua/

2) Захист корпоративної мережі та електронної пошти від вірусних атак і спаму[1] є наступною проблемою, вирішувати яку доводиться будь-якій промисловій компанії. Якщо з антивірусними рішеннями все вже більш-менш відомо, то питання фільтрації наявного спаму та захисту від нього стає все більш болючим з кожним днем – кількість спаму зростає практично експоненціально кожен рік! Згідно з останніми дослідженнями [5], спам становить близько 93-97 % від загального поштового трафіку в світі. Втрати від спаму, при всій своїй неочевидності, так само істотні: насамперед, багато компаній не мають безлімітного під'єднання до мережі Інтернет і платять за обсяг споживаного трафіку; другий бік спам-розсилок – втрати в робочому часі, який співробітники компаній витрачають, займаючись його фільтрацією на корпоративній поштовій скриньці. У цьому випадку засобами захисту від спаму є антивірусні-антиспамові системи [13]. Вони займаються фільтрацією спаму і забезпечують захист від шкідливого ПЗ і небажаної реклами. Програмні рішення такого класу пропонують багато виробників, а деякі пропонують як послугу – антиспам-рішення.

Якщо зовсім недавно основною операційною системою в світі була Windows, то тепер на зміну їй прийшла нова різноманітність програмних платформ. Розробники шкідливого ПЗ активно користуються цією ситуацією, придумуючи нові неприємні сюрпризи для працівників відділу ІТ та служби ІБ промислових компаній [9]. Незахищені комп'ютери схильні до атак різного шкідливого ПЗ, яке поширюється мережею Інтернет [2]. Шкідливе ПЗ (англ. malware, malicious software – шкідлива програма) – будь-яке ПЗ, призначене для отримання несанкціонованого доступу до обчислювальних ресурсів самого комп'ютера або до інформаційних ресурсів, які зберігаються на ньому, призначене для несанкціонованого власником їх використання чи спричинення шкоди (нанесення збитку) власникові комп'ютера, інформації чи комп'ютерній мережі шляхом копіювання, спотворення даних, видалення або підміни інформації.

Надійні технології захисту від шкідливого ПЗ вже довели свою ефективність поєднання традиційних, проактивних і хмарних методів їх виявлення [13]. Зокрема, фішинг-фільтр IE8 SmartScreen [2] ідентифікує і блокує сайти, які поширюють потенційно небезпечне ПЗ. Робота функції SmartScreen базується на репутації загроз, тобто дає змогу блокувати нові загрози, які виходять від наявних небезпечних сайтів, навіть якщо ці загрози не блокуються звичайним антивірусом або сигнатурами антивірусного ПЗ. Таким чином, фільтр SmartScreen доповнює звичайні антивіруси, забезпечуючи додаткові заходи безпеки і для ідентифікації, і для захисту. Однак, для всеосяжного захисту від шкідливого ПЗ потрібно також встановлювати традиційні антивірусні програми і періодично оновлювати їх.

Фільтр SmartScreen забезпечує блокування і під час пошуку, і при завантаженні файлу. Такий ступінь контролю дає змогу блокувати небезпечні

[1] Спам (англ. spam) – масове розсилання кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін "спам" стосується рекламних електронних листах. Також вважаються спамом освідчення в коханні на електронну пошту, в чатах, соціальних мережах і т.п.

сайти, окремі їх частини і потенційно небезпечні завантаження на звичайних сайтах. Цей фільтр збирає статистику шкідливого ПЗ, комбінуючи дані, отримані від компанії Microsoft, і тих, що надходять з інших джерел, забезпечуючи цим самим всебічний захист корпоративної мережі. Хоча він і уможливлює роботу користувача в браузері максимально безпечною, проте тут має працювати група фахівців, які займатимуться виключно питаннями вивчення й удосконалення захисту браузера.

3) Наступне завдання для забезпечення захисту інформації всередині промислової компанії – контроль споживаного Веб-трафіку, його оптимізація і захист від зовнішніх атак з мережі Інтернет. Тут існують переважно два напрямки захисту корпоративної мережі:

- система якісного захисту від атак ззовні, що відстежує спроби мережевих атак і захищає від розкриття інформації з корпоративних серверів;
- система розподілу доступу в мережі Інтернет з можливістю контролю обсягу інформації, її характеру, обмеження доступу до конкретних ресурсів і зменшення можливості скачування різної інформації.

Вирішення цього виду загроз – впровадження proxy-серверів або корпоративних брендмауери[1]. Найбільш відомими продуктами є CheckPoint Firewall[2], ISA Server[3] та ін. Наприклад, за допомогою брандмауера Windows можна запобігти проникненню через мережу Інтернет на сервер чи комп'ютер компанії хакерів або шкідливого ПЗ (наприклад, хробаків). Окрім цього, брандмауер запобігає надсиланню шкідливого ПЗ із комп'ютера компанії на інші комп'ютери. У брандмауер Windows вбудований журнал безпеки, який дає змогу фіксувати ip-адреси і інші дані, що відносяться до з'єднань в локальних і корпоративних мережах або в мережі Інтернет. Можна записувати як успішні під'єднання, так і пропущені пакети. Це дає змогу відстежувати, коли комп'ютер у мережі під'єднується, наприклад, до web-сайту. Ця можливість за замовчуванням відімкнута (її може увімкнути тільки системний адміністратор).

4) Ще один напрямок захисту мережевих інформаційних ресурсів – моніторинг за використанням та під'єднанням комп'ютерів і пристроїв всередині корпоративної мережі. Сьогодні цей аспект ІБ стає актуальним з таких причин:

- несанкціонований доступ працівників компанії в корпоративну мережу призводить до ризику втрати конфіденційної інформації;
- пристрої постійно додають і видаляють з корпоративної мережі без повідомлення ІТ персоналу;

[1] Брандмауер Windows – вбудований в Microsoft Windows міжмережевий екран. З'явився в Windows XP Sp2. Однією з відмінностей від попередника (Internet Connection Firewall) є контроль доступу програм в мережу. Брандмауер Windows є частиною Центру забезпечення безпеки Windows. Вбудовано у Windows Vista та Windows 7.

[2] Check Point FireWall – технологія перевірки з урахуванням стану протоколу (Stateful Inspection Technology), яка реалізує всі необхідні можливості firewall на мережевому рівні.

[3] Microsoft Forefront Threat Management Gateway (Forefront TMG), раніше відомий як Microsoft Internet Security and Acceleration Server (ISA Server) – проксі-сервер для захисту мережі від атак ззовні, а також контролю інтернет-трафіку, що описується Microsoft як Forefront TMG, ддає змогу співробітникам компанії безпечно і ефективно користуватися ресурсами.

- санкціонований доступ різних користувачів до пристроїв мережі, що не задовольняють політиці ІБ компанії, може призвести до негативних наслідків;

Оскільки сучасна корпоративна мережа – складне динамічне середовище, яке складається з різних пристроїв, таких як робочі станції, сервери, принтери, точки бездротового доступу, VoIP-телефони, комутатори, маршрутизатори та ін., то деякі компанії здатні вести докладний і деталізований облік обладнання та ПЗ в мережі. Однак, тільки маючи повне уявлення про всі пристрої в мережі, можна керувати ними і захищати локальну мережу від загроз ІБ. Для контролю пристроїв, які можуть працювати у корпоративній мережі, а також управління пристроями, які постійно під'єднують до мережі, на предмет виконання корпоративної політики ІБ (наприклад, запущеного і оновленого антивіруса) використовуються рішення класу Network Access Control.

Зокрема, система Symantec Network Access Control представляє собою комплексне рішення щодо контролю доступу до мережі, яке дає змогу компаніям ефективно і безпечно контролювати доступ користувачів до корпоративних мереж за допомогою інтеграції її з наявними мережевими інфраструктурами. Система збирає дані та оцінює стан відповідності кінцевих точок, забезпечує відповідний доступ до мережі, при потребі виправляє проблеми, що виникли, і безперервно відстежує зміни в стані відповідності кінцевих точок незалежно від того, як саме вони під'єднані до мережі. Внаслідок цього формується мережеве середовище, яка дає компаніям-підрядникам можливість істотно знизити кількість пригод, пов'язаних з порушенням ІБ, і забезпечити більш високий рівень відповідності вимогам корпоративної політики безпеки IT-інфраструктури.

Система Symantec Network Access Control також забезпечує легке і рентабельне розгортання та управління засобом контролю доступу до корпоративної мережі. У цьому сегменті рішень з ІБ доцільно використати такі продукти, як Miscosoft NAP[1] на базі Microsoft Exchange Server 2013, Cisco NAC, Kaspersky NAC і ін. Наприклад, забезпечення IT-безпеки корпоративної мережі будь-якої компанії стає нелегким завданням, коли в межах однієї мережі з'являються робочі станції та інші пристрої, що працюють на різних платформах і з різними операційними системами. Kaspersky Work Space Security пропонує захист робочих станцій, ноутбуків і смартфонів у мультиплатформових корпоративних мережах. Зокрема, програми інших виробників можна помістити в список довірених додатків, після чого вони будуть вилучені з перевірки. Це дає змогу підвищити продуктивність системи захисту, пришвидшити роботу антивірусного додатку і уникнути можливих конфліктів.

Інформаційна безпека є необхідною умовою ефективної роботи будь-якої компанії, проте захист великої корпоративної мережі є непростим завданням. Тому в Kaspersky Work Space Security входить Kaspersky Administration Kit[1] – єдине рішення для ефективного і зручного управління системою захисту всіх вузлів великої мережі. Він забезпечує відповідність стану антивірусного захисту вузлів корпоративної мережі політикам безпеки Cisco Network Admission Control (NAC). Продукт також повністю інтегрується з Microsoft Network Access Protection (NAP). Універсальний засіб управління Kaspersky Administration Kit дає змогу здійснювати централізований захист кінцевих користувачів, забезпечує зручне управління IT-безпекою і заощаджує час на моніторинг значної кількості вузлів корпоративної мережі.

[1] Network Access Protection (NAP) – захист доступу до мережі. Технологія компанії Microsoft, призначена для контролю доступу до мережі компанії, виходячи з інформації про стан системи комп'ютерів, що під'єднуються. Вперше технологія була реалізована в Windows XP Service Pack 3, Windows Vista і Windows Server 2008.

За допомогою Kaspersky Administration Kit системний адміністратор може здійснювати встановлення, налаштування та управління системою захисту корпоративної мережі, а також оперативно реагувати на події, які потребують втручання, не залишаючи свого робочого місця. Завдяки високій масштабованості системи захисту корпоративна мережа компанії залишається захищеною навіть при її інтенсивному зростанні. Kaspersky Administration Kit дає змогу вибудовувати ієрархію серверів адміністрування, забезпечуючи оптимальний розподіл навантаження між серверами, знижуючи навантаження на основний сервер, спрощуючи роботу з віддаленими офісами і даючи можливість розмежувати сфери відповідальності адміністраторів системи безпеки.

5) Наступною актуальною для багатьох промислових компаній проблемою є моніторинг дій системних адміністраторів, що мають фактично необмежені повноваження в інформаційних системах. Адже найчастіше для зламування системи достатньо просто знайти спільну мову з адміністратором або ж зацікавити його, скажімо, матеріально чи шантажем. Водночас і самі системні адміністратори нерідко є джерелами витоків конфіденційної інформації.

Для моніторингу дій співробітників, що забезпечують працездатність інформаційних систем і мають необмежені системні привілеї, використовуються спеціальні системи, наприклад, Balabit Shell Control Box[2], яка дає змогу здійснювати моніторинг з таких питань, як:

- веде спостереження і аудит роботи адміністраторів систем;
- здійснює контроль SSH, RDP і Telnet з'єднань;
- здійснює збір надійної інформації для можливих розслідувань;
- забезпечує керований контроль доступу до серверів;
- авторизація "Four eye" для запобігання людських помилок;
- ідентифікація серверів, що захищаються.

6) Для моніторингу та контролю дій користувачів існує цілий набір засобів. Програмні рішення такого класу представляють такі продукти, як Spec-

[1] "Антивирусы" Kaspersky Work Space Security. [Електронний ресурс]. – Доступний з http://ss-shop.com.ua / main/antivirusi.html?p=91

[2] Shell Control Box (SCB) – це інструмент (пристрій) для інспекції адміністративних протоколів, який може використовуватися для контролю та аудиту вилученого доступу до системи. Він може записувати і відтворювати дії системних адміністраторів, які керують серверами віддалено через SSH, RDP, Telnet, або VNC протоколи. SCB доступний як апаратний або віртуальний пристрій. Shell Control Box може відправляти списки відкритих та/або переміщених файлів зовнішньому DLP-рішенням. Водночас, рішення щодо запобігання витоків даних розпізнає, аналізує, відстежує і попереджає про доступ або передачу важливої інформації.

torSoft і LanAgent[1]. Ці програми призначені для прихованого спостереження за комп'ютерами в локальній корпоративній мережі. Вони здійснюють моніторинг активності користувача на будь-якому комп'ютері, під'єднаному до мережі компанії, а також дають змогу виявити діяльність тих, хто немає відношення до роботи самої компанії. Як звіти про їхню роботу, програми роблять знімки екранів комп'ютерів, ведуть докладні журнали натиснень клавіш, відвідувань сайтів у мережі Інтернет, листувань по ICQ, Jabber[2] чи електронною поштою і т.п.

Наприклад, додаток Spector 360 [1] є флагманським продуктом фірми SpectorSoft, призначений для централізованого моніторингу співробітників компанії. Він видає багаторівневу картину того, як співробітники компанії використовують свої робочі комп'ютери та мережу Інтернет. Додаток дає змогу інспектувати діяльність всієї компанії за допомогою простих у використанні графічних діаграм. У будь-який час керівник компанії може детально вивчити всіх дії своїх співробітників, щоб дізнатися про них більше, ніж вони це афішують.

Додаток Spector 360 містить в собі засоби для автоматичного розгортання, віддаленого управління та здійснює запис різноманітних дій, в т.ч.: E-mail, чати, миттєві повідомлення, відвідуванні веб-сайтів, он-лайнові пошукові запити, клавіші, що натискаються, і використовувані програми. Він також містить засіб для запису образів екрану в режимі відеокамери. За допомогою цього додатку можна згенерувати високоякісні звіти для керівництва, які можуть регулярно роздруковуватися або розсилатися поштою. Spector 360 розроблений для комерційних, освітніх і урядових організацій, які використовують корпоративні чи локальні мережі на платформі Windows.

Для віддаленого спостереження за персоналом в корпоративній мережі використовується програма LanAgent Standard[3]. Вона здійснює моніторинг активності на будь-якому комп'ютері, під'єднаному до мережі компанії, виконувані такі дії: перехоплює натиснення клавіш; запам'ятовує запуск і закриття програм; робить знімки екрану (скріншоти); стежить за вмістом буфера обміну; здійснює моніторинг файлової системи; реєструє відвідані сайти; відстежує з'єднання з мережею Інтернет.

Висновки. Реалії сучасної компанії – це доступ до корпоративної мережі з будь-якої точки світу, використання співробітниками особистих мобільних пристроїв, вільне переміщення конфіденційних даних усередині корпоративної мережі і за її межами, що спричиняє за собою серйозні ризики з точки зору корпоративної безпеки, – зазначив Олександр Савушкін [13], керуючий директор "Лабораторії Касперського" в Україні, Молдові і Республіці Білорусь. Одного антивірусного захисту вже недостатньо для забезпечення ІБ бізнесу компанії, адже мобільна революція та ускладнення ІТ-середовища вимагають кардинально нового способу його захисту. Сучасні досягнення в галузі ІТ та ІБ для потреб різних організацій і промислових компаній повністю відповідають потребам сучасного бізнесу, за допомогою нових і оновлених технологій забезпечують кращий захист корпоративних мереж та інформаційних ресурсів, а також вирішують таку поширену проблему ІТ-безпеки, як складність управління ІБ.

Керівникам, відповідальним за ІБ корпоративних мереж промислових компаній доводиться враховувати дуже багато аспектів захисту інформації, а також знати, за допомогою яких засобів може забезпечуватися реалізація тих чи інших завдань ІБ. Тільки комплексний підхід до вирішення проблем зовнішньої та внутрішньої ІБ компанії дасть змогу її керівнику бути впевненим у тому, що конфіденційна інформація не потрапить до компаній-конкурентів чи різних зловмисників і не завдасть шкоди самій компанії.

[1] LanAgent Standard Версия 2.5. [Електронний ресурс]. – Доступний з http://nnm.ru/blogs/vikamanunaj/lanagent_ standard_versiya_2_5/

[2] Сучасна структура спілкування в мережі Інтернет дуже розвинена і багатогранна. Користувачеві доступно безліч видів спілкування, таких як чати, пошта, аудіо- та відео- конференції, форуми, соціальні мережі і т.д. Проект Jabber – популярний у вільному і відкритому протоколі для спілкування за допомогою миттєвої відправки та отримання текстових повідомлень в мережі Інтернет. Цей проект задуманий як набір простих інструкцій, окремо для "чайників" і середньокваліфікованих користувачів, які дадуть змогу швидко почати використовувати Jabber і, як наслідок, робити це безпечно і з комфортом.

[3] Сергеев Юрий / LanAgent: удалённое наблюдение за персоналом по сети / Юрий Сергеев. [Електронний ресурс]. – Доступний з http://inet-press.mylivepage.ru/wiki/3/3

Література

1. Spector 360. [Electronic resource]. – Mode of access http://cbit.ua/ru/sredstva-kontrolya-i-monitoringa-spector-soft-/?content_id=392&lang_id=1&product_id=124

2. Безпека IE8: захист від шкідливого ПЗ за допомогою фільтра SmartScreen. [Електронний ресурс]. – Доступний з http://easy-code.com.ua/2011/02/bezpeka-ie8-zaxist-vid-shkidlivogo-pz-za-dopomogoyu-filtra-smartscreen/

3. Бєгун А.В. Інформаційна безпека / А.В. Бєгун. – К. : Вид-во КНЕУ, 2008. – 280 с.

4. Герасименко О.В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О.В. Герасименко, А.В. Козак. [Електронний ресурс]. – Доступний з http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/

5. Глобальное исследование информационной безопасности. [Электронный ресурс]. – Доступный с http://www.gosbook.ru/node/64161

6. Глобальное исследование инцидентов внутренней информационной безопасности. [Электронный ресурс]. – Доступный с http://www.securitylab.ru/analytics/291018.php

7. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства / Г.С. Гриджук. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

8. Компании ищут способы оперативного реагирования на современные угрозы и больше не могут обеспечивать информационную безопасность путем решения отдельных задач. [Электронный ресурс]. – Доступный с http://www.ey.com/RU/ru/Newsroom/News-releases/Press-Release---2012-10-29-2.

9. Корпоративная информационная безопасность: виды IT-угроз. [Электронный ресурс]. – Доступный с http://www.razumny.ru/stat/it-ugrozy.html

10. Кунинець А.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / А.І. Кунинець, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.

11. Мониторинг утечек информации. [Электронный ресурс]. – Доступный с http://www.infowatch.ru/analytics/leaks_monitoring

12. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal / Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

13. Час антивірусів пройшло: "Лабораторія Касперського" представляє корпоративну захист нового покоління. [Електронний ресурс]. – Доступний з http://www.infoportal.pp.ua/news/chas_antivirusiv_projshlo_laboratorija_kasperskogo_predstavljae_korporativnu_zakhist_novogo_pokolinnja/2013-02-27-1742#.UVad0leqa70

14. Чудінова Н.В. Особливості використання мережі Інтернет для отримання конфіденційної інформації / Н.В. Чудінова, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.3. – С. 337-346.

Милян К.В., Грыцюк Ю.И. **Особенности организации информационной безопасности корпоративной сети промышленной компании**

Рассмотрены особенности организации информационной безопасности (ИБ) корпоративной сети промышленной компании, которая позволяет их руководителям убедиться в том, что конфиденциальная информация не попадет к злоумышленникам или в руки компаний-конкурентов и, как следствие, не нанесет вреда самой компании. Выяснено, что реалии современного бизнеса – это доступ соответствующих работников компании к ее информационным ресурсам из любой точки местонахождения, использование ими личных мобильных устройств для свободного перемещения конфиденциальных данных внутри корпоративной сети и за ее пределами, что приводит к серьезным рискам обеспечения безопасности хозяйственной деятельности компании. Поэтому руководителям служб ИБ корпоративных сетей компаний приходится учитывать многие особенности защиты информации, а также знать, с помощью каких средств может обеспечиваться реализация тех или иных задач ИБ.

Ключевые слова: информационные угрозы, информационная безопасность, информационные технологии, источники угроз, промышленная компания.

Milyan K.V., Grycyuk Yu.I. **Features of the organization of information security corporate network industrial company**

The features of the organization of information security (IS) industrial company intranet, which allows their managers to make sure that sensitive information does not fall into the hands of criminals or of competing companies and, as a consequence, will not harm the company. It was found that the realities of modern business – access of the employees of the company to its information resources from anywhere in the location, the use of personal mobile devices for free movement of sensitive data on the corporate network and beyond, leading to serious security risks of the company's operations. Therefore, managers corporate information security network companies have to consider many aspects of information security, and to know by what means can be provided by the implementation of certain tasks IS.

Keywords: information threats, information security, information technology, threat sources, industrial company.

УДК 658.[5.011.4+011.56]

Доц. В.І. Блонська, канд. екон. наук;
магістрант А.О. Пальчук – Львівська КА

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЕФЕКТИВНОГО ОЦІНЮВАННЯ СТРАТЕГІЧНОГО ПОТЕНЦІАЛУ ПІДПРИЄМСТВА

Розглянуто основні функції автоматизованої системи підтримки прийняття управлінських рішень. Охарактеризовано цінові позиції на інформаційні системи, що представлені на вітчизняному ринку. Проведено огляд можливостей використання систем бізнес-планування для оцінювання економічного потенціалу підприємств. Визначено етапи впровадження інформаційних систем для ефективного управління підприємствами.

Ключові слова: інформаційні технології, інформаційні системи, програмне забезпечення, стратегічний потенціал підприємства.

Актуальність теми. Оскільки процес ефективного управління діяльністю підприємства та розвитку його стратегічного потенціалу має забезпечити можливість його рентабельного функціонування в ринковому середовищі, виникає необхідність використання оптимальних інформаційних технологій, що передбачає застосування інноваційного підходу до управління та організації діяльності підприємства, для забезпечення оперативності й обґрунтованості прийняття управлінських рішень. З огляду на це, виникає потреба в організації інформаційного забезпечення управління ефективністю функціонування підприємства та адаптації візуально-моніторингових програмних продуктів до сучасних умов його господарювання в Україні.

Аналіз останніх досліджень та публікацій. Питання застосування інформаційних технологій для прийняття управлінських рішень щодо діяльності підприємств широко розглядають зарубіжні та вітчизняні науковці, а також застосовуються у практичній діяльності підприємств. Значні здобутки у вивченні цієї проблеми мають такі дослідники: І. Богдан, А. Гончарук, С. Гераськів, С. Дмитріев, А. Жевага, Ю. Орлов, Е. Попов, В. Ситник, В. Дунаєв, М. Тарасюк, Д. Хан, Х. Хунгенберг, В. Шумов та інші. Поряд з цим, питання удосконалення економічного оцінки стратегічного потенціалу, зокрема в аспекті організації його інформаційного забезпечення, залишається дискусійним і підлягає подальшому дослідженню.

Постановка завдання. Дослідити питання використання сучасних інформаційних технологій для ефективної оцінки стратегічного потенціалу підприємства.

Виклад основного матеріалу. У сучасних умовах господарювання та у контексті розвитку ринку інтелектуальних ресурсів у сфері управління, для підвищення рівня управління ефективністю функціонування підприємства важливим є застосування інтелектуальних інформаційних технологій, а саме візуально-моніторингового програмного продукту.

Особливу увагу потрібно приділяти застосуванню інформаційних технологій для оптимізації процедур функціонування й побудови процесно орієнтованих систем керування підприємствами, що розглядають його функціонування не з погляду реалізації окремих функцій, а з позицій виконання цілісних процесів як сукупності процедур бізнес-процесів. На цій основі повинен бути представлений комплекс оптимізованих моделей і методів керування підприємствами, а також сформульований загальний підхід до оптимізації процедур бізнес-процесів [4, с. 5].

Функції автоматизованої системи підтримки прийняття управлінських рішень щодо ефективності управління стратегічним потенціалом для сучасного підприємства передбачають:

- введення та коригування інформації, необхідної для вирішення завдань;
- розрахунок показників економічного потенціалу підприємства, маркетингового його комплексу, зовнішнього і внутрішнього середовища;
- контроль реалізації стратегії й тактики управління розвитком підприємства;
- генерація регулювальних дій за відхилення показників розвитку підприємства від планових значень;
- консультація щодо сформованої ситуації;
- формування прогнозу розвитку ситуації до і після реалізації регулювальних дій;
- оцінювання доцільності та ефективності регулювальних дій.