Секція 2
"Проблеми розвитку підприємництва в Україні в умовах європейської інтеграції"

2.2. Проблеми обліку, аналізу та аудиту

УДК 330.75

Данилюк І. В.

Голяш І. Д.

ВИКОРИСТАННЯ АУДИТОРСЬКИХ ПРОЦЕДУР З МЕТОЮ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

Анотація. Розглянуто види аудиту інформаційної безпеки, подано їх характеристики, зазначено переваги та недоліки. Визначено, що аудит інформаційної безпеки необхідно розглядати як системний процес оцінок поточного стану інформаційної системи з визначеними аспектами захисту.

Аннотация. Рассмотрены виды аудита информационной безопасности, поданы их характеристики, отмечены преимущества и недостатки. Определенно, что аудит информационной безопасности необходимо рассматривать как системный процесс оценок текущего состояния информационной системы с определенными аспектами защиты.

Annotation. The types of audit of informative safety are considered, their descriptions are given, advantages and failings are marked. It is certained that the audit of informative safety must be examined as a system task of estimations of current status of the informative system with the certain aspects of defence.

Ключові слова: аудиторська процедура, корпоративна інформація, інформаційна безпека.

Тривалий час розуміння аудиту інформаційної безпеки в наукових джерелах ототожнювалося тільки з безпекою інформації, що значно звужувало її сутність. Саме тому з низки питань, присвячених розгляду проблеми забезпечення інформаційної безпеки підприємств, найбільш вивченими та дослідженими її аспектами є безпека інформації (інформаційно-технічна безпека).

Проблема розробки систем аудиту інформаційної безпеки у вітчизняній науковій літературі достатньо ґрунтовно не досліджувалась. Вона розглядалася лише через висвітлення окремих її аспектів вітчизняними та зарубіжними фахівцями. У цьому контексті слід згадати наукові розробки таких вчених, як: В. Артемов, І. Бачило, К. Бєляков, В. Богуш, В. Брижко, В. Гавловський, В. Голубєв, В. Горобцов, С. Комов, Н. Кушакова, А. Марущак, В. Петренко, В. Цимбалюк, І. Чиж, В. Ярочкін та ін.

Мета статті – теоретико-методологічне обґрунтування суті інформаційної безпеки, аналіз різних видів аудиту інформаційної безпеки підприємства та дослідження ефективної системи захисту корпоративної інформації за результатами аудиту.

Аудит безпеки дозволяє перевірити, наскільки добре захищена інформаційна система підприємства від внутрішніх і зовнішніх загроз. Регулярний аудит дозволяє підтримувати систему інформаційної безпеки на належному рівні, вчасно виявляти потенційні проблеми, контролювати дотримання правил і норм політики безпеки, встановленої на підприємстві.

Тестування на проникнення – вид аудиту інформаційної безпеки, що дозволяє виявити зовнішні загрози, до яких схильні Інтернет-ресурси підприємства. У ході аудиту проводиться комплексне обстеження серверів, підключених до мережі Інтернет, виявляються уразливі місця і помилки конфігурації, використовуючи які можна здійснити проникнення на сервер ззовні, дістати несанкціонований доступ до критичної інформації, порушити її цілісність і доступність.

Внутрішній аудит інформаційної безпеки – вид аудиту, що вимагає фізичної присутності аудиторів на досліджуваному об'єкті. Фахівці проводять співбесіду з керівниками підприємства різних рівнів, вивчають специфіку бізнес-процесів підприємства, структуру інформаційної системи, правила розмежування доступу, існуючу внутрішню документацію, що регламентує правила і норми роботи з конфіденційною інформацією. Проводиться тестування захищеності інформаційної системи від внутрішніх загроз (включаючи людський фактор), перевіряються налаштування серверів і комп'ютерних робочих місць підприємства, перелік дозволеного до використання програмного забезпечення, наявність оновлень і патчів, ефективність роботи захисних засобів – антивірусів, міжмережевих екранів, антишпіонських програм та ін. Перевіряється політика резервного копіювання, методи зберігання інформації та її захищеності від непередбачених втручань.

При проведенні аудиту аудитор повинен використовувати рекомендації міжнародних стандартів у поєднанні з власними методиками, що розроблені протягом років роботи і постійно вдосконалюються з урахуванням сучасних реалій і загроз. Частина робіт із зовнішнього аудиту повинна бути автоматизованою за допомогою новітніх продуктів виробництва, що дозволить за короткий час перевірити систему на стійкість до десятків тисяч відомих атак. Інша, більш складна частина робіт, може виконуватись вручну із застосуванням досвіду та знань експертів для здійснення безпечних проникнень у досліджувані системи і для вироблення рекомендацій та інструкцій щодо усунення виявлених вразливостей систем захисту.

Можна виділити такі основні види аудиту інформаційної безпеки:

експертний аудит безпеки, у процесі якого виявляються недоліки в системі заходів захисту інформації на основі наявного досвіду експертів, що беруть участь у процедурі обстеження;

оцінка відповідності рекомендаціям Міжнародних стандартів;

інструментальний аналіз захищеності АС, направлений на виявлення й усунення "слабких місць" програмно-апаратного забезпечення системи;

комплексний аудит, що включає всі вищеперелічені форми проведення обстеження.

Кожний з вищеперелічених видів аудиту може проводитися окремо або в комплексі, залежно від тих завдань, які необхідно вирішити підприємству. Як об'єкт аудиту може виступати як АС компанії в цілому, так і її окремі сегменти, в яких проводиться обробка інформації [1, с. 244].

Важливим елементом розвитку сучасних підприємств є автоматизація бізнес-процесів з упровадженням засобів обчислювальної техніки і телекомунікацій. Наслідком цього є неухильний підйом розмірів інформації, яка піддається обробці й скупченню в електронному вигляді.

З підйомом електронного документообігу підприємства зростає залежність його діяльності від безперервності функціонування інформаційної системи (ІС) як одного цілого і від збереження корпоративної інформації в процесі її обробки та збереження на електронних носіях.

Зростання інформаційної системи підприємства, що є неминучою частиною вдалого розвитку бізнесу, має на меті посилення вимог до безперервності її функціонування, а також до збереження і забезпечення конфіденційності корпоративної інформації. ІС підприємства перетворився з друкарської машини в інструмент ведення бізнесу, що, у свою чергу, втягує підприємство у все більшу залежність від уразливості, що постійно ускладнюється ІС.

Однією з критичних якостей уразливості ІС є недоступність плану заходів щодо відновлення її працездатності після кризи. У разі виникнення форс-мажорних подій можна орендувати нову будівлю, купити техніку, підключити телекомунікації, але неможливо повернути функціональність ІС, якщо втрачена інформація із спеціального засобу її обробки.

Результати аудиту дозволяють збудувати кращу за ефективністю і витратами систему захисту корпоративної інформації, адекватну поточним завданням і цілям бізнесу.

Дуже принципово усвідомлювати й обдумувати те, що:

забезпечення інформаційної безпеки – це безперервний процес, що пов'язав правові, організаційні і програмно-апаратні заходи захисту;

в основі цього процесу лежить періодичний аналіз безпеки інформаційної системи в розрізі подоб небезпек і динаміки їх розвитку;

інформаційна система, у власному розвитку, зобов'язана піддаватися періодичним реорганізаціям, відправною крапкою будь-якою з яких працює тест виявлених уразливостей під час виконання аудиту інформаційної безпеки.

Аудит інформаційної безпеки зобов'язаний бути націлений як на професіоналів у сфері області IT-забезпечення, так і на фахівців у сфері менеджменту. Такий розклад позбавляє наявне нерозуміння фахівців у сфері інформаційної безпеки TOP-менеджерами компанії.

Для перевірок ефективності й безпечності інформаційної системи як такої здійснюють комп'ютерний аудит інформаційної системи. Під ним мається на увазі оцінка поточного стану комп'ютерної системи на відповідність певному стандарту або запропонованим вимогам [2, с. 259]. Цей термін використовується, насамперед, спеціалістами з загальної безпеки комп'ютерних інформаційних систем і у вузькому значенні не стосується аудиту фінансової звітності. Такий аудит не спрямований на пропонування конкретного рішення, він дає можливість поглянути на інформаційну систему комплексно, виявити проблемні місця, сформувати обґрунтовані рекомендації для ухвалення рішення про усунення недоліків, а також включає декілька напрямів (рисунок).

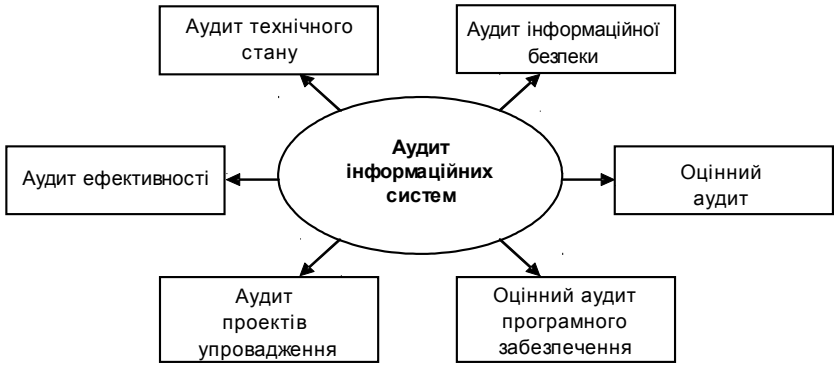

Рис. **Напрями аудиту інформаційних систем**

Аудит ефективності інформаційної системи дає можливість підприємству оцінити сукупну вартість володіння інформаційною системою і порівняти показники досліджуваної системи з лідером у цій галузі,

а також оцінити терміни повернення інвестицій при вкладенні коштів в інформаційну систему, розробити оптимальну схему вкладень, здійснити ефективне витрачання коштів на обслуговування й підтримку, знизити виробничі витрати. Цей вид аудиту включає такі частини інформаційної системи підприємства, як апаратні засоби, програмне забезпечення, периферійні пристрої, IT-персонал компанії, а також документи, бізнес-процеси, інформаційні потоки, користувачі.

Здебільшого комп'ютерний аудит інформаційних систем потрібний, якщо автоматизована система призначена для обробки конфіденційної чи секретної інформації. Але саме до таких належать комп'ютерні системи фінансового обліку. Проведення комп'ютерного аудиту корисно також після побудови автоматизованої системи та її підсистеми безпеки на етапі приймання в експлуатацію для оцінки ступеня дотримання висунутих до неї вимог [3, с. 159].

Отже, аудит інформаційної безпеки − це системний процес здобуття неупереджених високоякісних і кількісних оцінок поточного стану корпоративної інформаційної системи в узгодженні з певними аспектами захисту, основними завданнями якого є справедливо розцінити поточний стан інформаційної безпеки компанії, а також її адекватність поставленим цілям і завданням бізнесу щодо збільшення ефективності і рентабельності фінансової діяльності компанії.

Література: 1. Бутинець Ф. Ф. Аудит: стан і тенденції розвитку в Україні та світі : монографія / ред. проф. Ф. Ф. Бутинець, Н. М. Малюга, Н. І. Петренко. – Житомир : ЖДТУ, 2004. – 564 с. 2. Щербакова Н. С. Аудит інформаційної безпеки : навч. посібн. / Н. С. Щербакова. – Харків : Ескада, 2004. – 328 с. 3. Івахненков С. В. Комп'ютерний аудит: контрольні методики і технології : наукове видання / С. В. Івахненков. – К. : Знання, 2005. – 286 с. 4. Аглицький І. В. Інформаційні технології і бізнес : навч. посібн. / І. В. Аглицький. – К. : Знання, 2002. – 341 с. 5. Завгородній В. П. Автоматизація бухгалтерського обліку, контролю, аналізу та аудиту / В. П. Завгородній. – К. : А.С.К., 2004. – 768 с. 6. Клименко О. В. Інформаційні системи і технології в обліку : навч. посібн. / О. В. Клименко. – К. : Центр учбової літератури, 2008. – 320 с. 7. Кондрашова С. С. Информаційні технології в управлінні : навч. посібн. / С. С. Кондрашова. – К. : МАУП. 2007. – 250 с. 8. Крилов І. В. Інформаційні технології: теорія і практика : навч. посіб. / І. В. Крилов. – М. : Центр, 2006. – 530 с. 9. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій : навч. посібн. / В. М. Петрик, В. В. Остроухов та ін. – К. : Росава, 2006. – 208 с. 10. Сухоруков А. І. Пріоритети інвестування інформаційно-технологічного розвитку / А. І. Сухоруков // Стратегічна панорама. – 2008. – № 1. – 150 с. 11. Чубатенко О. І. Інформаційні технології – майбутнє України / О. І. Чубатенко // Дзеркало тижня. – 2007. – № 1. 12. Weber R. Information systems control and audit / R. Weber. – Upper Saddle River, Prentice-Hall, Inc., 2001. – 1013 p.

УДК 336.6

Яремченко Л. М.

ОСОБЛИВОСТІ КРЕДИТНОЇ ПІДТРИМКИ МАЛОГО ПІДПРИЄМНИЦТВА БАНКАМИ УКРАЇНИ

Анотація. Розглянуто проблему кредитування малого підприємництва, що є однією з головних серед проблем державної підтримки даного сектору економіки.

Аннотация. Рассмотрена проблема кредитования малого предпринимательства, которая является одной из главных среди проблем государственной поддержки данного сектора экономики.

Annotation. Crediting of small businesses is suggested to be one of the major issues of state support of this sector of economy.

Ключові слова: мале підприємництво, державна підтримка, кредитування, кредитна програма.

Невід'ємною складовою державної політики сприяння розвитку підприємництва в Україні є державна підтримка малого підприємництва, яка здійснюється в різних формах відповідно до діючих програм. Відповідно до законів України "Про державну підтримку малого підприємництва" [1] та "Про Національну програму підтримки малого підприємництва" [2] визначені такі програми сприяння розвитку малого підприємництва, як: формування інфраструктури підтримки і розвитку малого підприємництва; надання фінансово-кредитної та інвестиційної підтримки; організація підготовки та перепідготовки кадрів; встановлення системи пільг; запровадження спрощеної системи оподаткування. Проте банківське кредитування є одним із пріоритетних напрямів державної підтримки малого підприємництва, адже воно забезпечує залучення початкових фінансових ресурсів як для створення власної справи, так і фінансове забезпечення малих підприємств протягом усього його життєвого циклу.

Проблеми державної підтримки малого підприємництва, зокрема їх кредитування, в теоретичному та практичному аспектах розкриті у працях Варналія З. С., Дриги С. Г., Фастовець М. М., Воротіної Л. І., Рубе В. А., Реверчука С. К., Демченко В. О., Кривицької Н. Ю. та Зілгалової О. А.