6. Рощаховский А.К. Балансы акционерных предприятий. – С.-Пб.: Типо-Литография "Якорь", 1910. – С.18.
7. Вейцман Р.Я. Курс счетоводства (двойная бухгалтерия и ее применение к различным видам хозяйств). 16-е изд. значительно дополненное. – М.: Издание Центросоюза, 1929. – С.26.
8. Бадер В. Капітал і фонди // Економіка України. – 1992. – №7. – С. 39.
9. Струмилин С.Г. Избранные произведения. Т. 1. Статистика и экономика. – М.: Издательство академии наук СССР, 1963. – С. 30.
10. Хикс Дж.Р. Стоимость и капитал: Пер. с англ./ Общ. ред. и вступ, ст. Р.М. Энтова. – М.: "Прогресс", 1993. – С. 79.
11. Самуельсон Пол А., Нордхаус Вильям Д. Экономика: Пер. с англ. – М.: "Издательство БИНОМ", 1997. – С. 287.
12. Макконел К.Р., Брю С.Л. Экономикс: Принципы, проблемы и политика. В 2 т.: Пер. с англ. 11-го изд. – М.: Республика, 1992. – С. 37.
13. Нікбахт Е., Гроппеллі А. Фінанси / Пер. з англ. В.Ф. Овсієнка та В.Я. Мусієнка; – К.: Основи, 1993. – С. 19.
14. Принципы бухгалтерского учета /Б. Нидлз, Х. Андерсон, Д. Колдуел : Пер. с англ. / Под. ред. Я В Соколова. – М.: Финансы и статистика, 1993. – С.263.
15. Хендриксен Э. С, Ван Бреда М.Ф. Теория бухгалтерского учета: Пер. с англ. / Под ред. проф. Я.В. Соколова. – М.: Финансы и статистика, 1997. – С. 480.
16. Бухгалтерський облік за національними стандартами. Практичний посібник. / Укладачі: Я.Д. Крупка, З.В. Задорожний, Р.О. Мельник. – Тернопіль: Економічна думка, 2000. – С 12.

***Неля Проскуріна**, к.е.н., доцент*
Запорізький національний університет
м. Запоріжжя, Україна

АУДИТОРСЬКІ ПРОЦЕДУРИ ПРИ ПРОВЕДЕННІ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В умовах трансформаційних процесів і глобалізації економіки інформація є одним із самих значущих ресурсів у будь-якій компанії, організації, підприємстві, а для деяких – і основним виробничим ресурсом, адже від збереження інформації й безперебійного доступу до неї нерідко залежать важливі технологічні й бізнес-процеси. Інформаційні технології впливають на виробничі процеси підприємств. [1] Для того щоб оцінити реальний стан захищеності ресурсів інформаційної системи і її здатність протистояти зовнішнім і внутрішнім загрозам безпеки, необхідно регулярно проводити аудит інформаційної безпеки.

Аудит інформаційної безпеки – це системний процес отримання об'єктивних якісних і кількісних оцінок щодо поточного стану інформаційної безпеки підприємства у відповідності з визначеними критеріями і показниками безпеки.

З приводу аудиту інформаційних систем у світі накопичений колосальний досвід. Він узагальнений відомої організацій ISACA (Information Systems and Control Associations) і сформований у вигляді відповідних нормативів і методик під загальною назвою COBIT (Control Objectives for Information and related Technologies – Завдання управління для інформаційних і пов'язаних з ними технологій).

Процес аудиту інформаційної безпеки підприємства повязують з такими етапами:

1) вивчення поточного стану й планів розвитку інформаційних технологій на підприємстві;

2) порівняння результатів з тим, як повинні працювати інформаційні системи в ідеальному(оптимальному) стані (тобто з відповідними стандартами в даній області);

3) розробка рекомендацій для підприємства – що необхідно зробити, щоб максимально наблизитися до зазначених стандартів.

У процесі планування та проведення аудиту інформаційної безпеки важливе значення має розуміння суті і призначення процедур аудиту:

- анкетування фахівців з окремих відділів управління;
- інтерв'ю із ключовими працівниками;
- вивчення наявної нормативної документації, організаційної структури, принципів управління інформаційною системою;
- аналіз вихідних даних про організаційну й функціональну структуру ІТС підприємства, необхідних для оцінки стану інформаційної безпеки;
- вибіркове або суцільне тестування апаратного забезпечення, продуктивності мережі;
- аналіз існуючої політики інформаційної безпеки на предмет повноти й ефективності;
- аналіз інформаційних і технологічних ризиків пов'язаних зі загрозами інформаційній безпеці;
- здійснення тестових спроб несанкціонованого доступу до критично важливих вузлів інформаційної системи і визначення уразливості в установках захисту даних вузлів;
- проведення відповідних експертних оцінок;
- формування рекомендацій з розробки (або доробки) політики на підставі аналізу існуючого режиму інформаційної безпеки;

- розробка рекомендацій з використання існуючих і установці додаткових засобів захисту інформації для підвищення рівня надійності безпеки підприємства.
- підготовка аудиторського звіту за результатами надання аудиторських послуг.

Аудит інформаційної безпеки можна розділити на два види:

1. Експертний аудит інформаційної безпеки. При проведенні аудиту виявляють недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь в аудиті. Мета проведення експертного аудиту інформаційної безпеки полягає в оцінці стану інформаційної системи і розробка рекомендацій із застосування комплексу організаційних заходів і програмно-технічних засобів, спрямованих на захист інформаційних та інших ресурсів інформаційної системи від загроз. Експертний аудит дозволяє прийняти обґрунтовані рішення з використання засобів захисту, оптимальних щодо їх вартості й можливості попередження загроз інформаційній безпеці.

2. Аудит інформаційної безпеки на відповідність міжнародному стандарту ISO/IEC27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги», розроблений Міжнародною організацією по стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) на основі британського стандарту BS 7799-2:2002 «Системи управління інформаційною безпекою. Специфікація й посібник із застосування». Даний вид аудит являє собою перелік вимог до системи менеджменту інформаційної безпеки (СМІБ), обов'язкових для сертифікації. Стандарт установлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки й удосконалювання документованої СМІБ у контексті існуючих бізнес – ризиків організації. [2]

Аудит містить у собі такі послідовні етапи виконання робіт з виростанням відповідних аудиторських процедур. (рис.1)

Об'єктом аудиту може виступати інформаційна система підприємства в цілому, і також її окремі сегменти, що забезпечують обробку інформації, яка підлягає захисту. Ми вважаємо, що аудит можна проводити як силами штатного персоналу (внутрішній аудит), і шляхом залучення незалежних фахівців (зовнішній аудит). Проте використання зовнішнього аудиту має такі переваги:

- являє собою незалежне дослідження, що підвищує рівень об'єктивності результатів;
- проводиться силами фахівців, не зв'язаних раніше з підприємством-замовником і тому мають неупереджений погляд на наявні проблеми, що автоматично підвищує достовірність результатів. [3]

Рисунок 1 Етапи аудиту інформаційної безпеки з виростанням відповідних аудиторських процедур

Залучення власних фахівців відриває їх від виконання основних обов'язків [4], що впливає на якість їх поточної роботи результатів аудиту:

- використання зовнішнього аудиту сприяє скороченню часу на аудиту і підвищує якість обробки запитів співробітників підприємства.
- використання апробованих методик дозволяє провести аудит швидко і якісно, що впливає на скорочення витрат на аудит й дозволяє підвищити рівень захищеності інформаційних технологій;
- проведення аудиту вимагає фахівців високої кваліфікації, що мають не тільки досвід роботи з найрізноманітнішим програмним і апаратним забезпеченням, й досвід проведення аудиту.

Результатом аудиту інформаційної безпеки є пакет документів, що містять деталізовані дані про стан мережі й рекомендацій з поліпшення якості роботи, підвищення надійності, продуктивності, захищеності й ефективності надання послуг. Зміст документації в значній мірі залежить від бажань підприємства, наявної інформаційно-технологічної інфраструктури та організаційної структури підприємства. [3]

Звітним документом про результати аудиту є аудиторський звіт Його призначення й структуру доцільно погоджувати між аудиторської фірмою і підприємством одночасно з визначенням мети аудиту інформаційної безпеки. [2]

В умовах зростаючих темпів розвитку бізнесу стають усе більше необхідними проведення аудиту інформаційних систем, методів і засобів безпеки і побудова моделей оцінки ризиків. В майбутньому, варто очікувати поступового злиття аудиту із процесом супроводу системи й перехід до аудиту на постійній основі.

Література:

1. Бородюк В. П. Повышение экономической эффективности системы информационной безопасности / В.П. Бородюк, А.В.Львова // Вестник МЭИ. – 2007. – №4. – С.139-142.
2. Подольский В.И. Компьютерный аудит: [Практ. пособие] / В.И.Подольский, Н.С., Щербакова, В.Л.Комиссарова; под. ред.. проф..В.И.Подольского. – М.: ЮНИТИ-ДАНА, 2004. – 128с.
3. Гришина Н. В. Организация комплексной системы защиты информации./ Н.В. Гришина.– М.: Гелиос АРВ. – 2007. – 256 с.
4. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв [та ін] ; заг. ред. Р. А. Калюжний ; Гуманітарний ун-т "Запорізький ін-т держ. та муніціпального управління". – Запоріжжя: Просвіта. – 2001. – С. 236-246.

***Наталія Різник**, к.е.н., доцент*
Луцький національний технічний університет
м. Луцьк, Україна

ЕТАПИ ФОРМУВАННЯ СТРАТЕГІЇ БЕЗПЕКИ БАНКУ

Невпинне зниження конкурентноздатності економіки України, зростання економічної залежності від кон'юнктури коливань світових ринків, поглиблення соціальних диспропорцій і зростання соціальної напруги породжують все нові ризики, загрози та небезпеки в розвитку банківської системи держави. Тому важливими завданнями сьогодення є розробка науково обґрунтованих підходів стратегічного забезпечення безпеки банківської системи.

В економічній теорії проблеми зміцнення безпеки банківських установ розглядалися такими вченими, як В.Ярочкін [1], В.Гамза, І.Ткачук [2], Є.Олєйніков [3], М.Єрмошенко [4], О.Барановський [5], Л.Стрельбицька,