ВСТУП

Запропонований вашій увазі підручник аналізує сучасний стан аудиту інформаційної безпеки (ІБ) організації, а також дає вичерпні відповіді та рекомендації на низку запитань, які виникають при його здійсненні, зокрема, навіщо проводити аудит, як проводити аудит, які процедури використовувати, до яких результатів може зумовити аудит, хто має право проводити таку перевірку, як оцінити результати аудиту тощо.

Нинішній етап розвитку суспільства має ту особливість, що на зміну індустріальному суспільству прийшло інформаційно-індустріальне, характерною рисою якого є визначальна роль систем розповсюдження, зберігання та оброблення інформації. Стрімко зростає кількість цінної інформації в інформаційних системах, від якості, достовірності та оперативності одержання якої залежить прийняття важливих рішень на різних рівнях – від президента держави чи організації до рядового громадянина. За своєю значимістю та актуальністю проблема інформатизації є найважливішою для сучасного суспільства. І дійсно, запровадження інформаційних технологій на основі новітніх засобів обчислювальної техніки та систем зв'язку зробило інформаційну сферу незамінним атрибутом сучасного суспільства, забезпечуючи його життєдіяльність і прискорений розвиток. А тому у підсумку *суспільство*, взагалі, і *громадянин*, зокрема, стають все більш залежними від *якості* функціонування *інформаційних систем та мереж*.

Зворотною стороною цих вкрай важливих та позитивних процесів є поява все нових та зростаючих **загроз** *порушення режиму* **безпеки інформації** у результаті виникнення та розвитку в інформаційних системах та мережах **інцидентів інформаційної безпеки** (ІІБ) [1–6]. Аналіз показує, що з часом *інциденти інформаційної безпеки* будуть набувати все більшого розмаху, а тому також буде *зростати залежність організації від інформаційних, комунікаційних систем та послуг*, які стають вразливішими до порушень режиму ІБ, що може зумовити втрату ***інформаційних активів*** організації та завдання їй збитків аж до згортання бізнесу.

При побудові системи управління ІБ організації, поряд з процесами оцінювання ризиків такої безпеки [7], реалізації та експлуатації заходів/засобів захисту, навчання персоналу основам ІБ та іншими важливими процесами, **визначальними для управління є процеси контролю та перевірки дотримання вимог ІБ**. Своєчасність, точність та повнота оцінок стану ІБ, які отримані у результаті *контролю та перевірки* організації, дають можливість *ідентифікувати*

вразливості системи менеджменту, *виявляти недооцінені ризики*, *визначати превентивні заходи*, що скеровані на удосконалення процесів забезпечення ІБ.

Серед *процесів контролю та перевірки* ІБ організації особливе становище займає **аудит інформаційної безпеки, основним призначенням якого є формування незалежного оцінювання стану ІБ організації, незалежної від діяльності, яка перевіряється**. Саме цю проблему ми будемо аналізувати у процесі вивчення дисципліни «Аудит інформаційної безпеки».

Поняття «**аудит інформаційної безпеки**» з'явилося відносно недавно. Натомість історія аудиту (від латинського слова *audire* – слухати) сягає часів Древнього Риму, коли постанови правителів розповсюджувалися за допомогою офіційних речників. Для того, щоб постанови зачитувалися речниками правильно, без перекручень, кожного з них супроводжував *аудитор*, тобто спеціальна людина, яка знала текст постанови і стежила, щоб речник правильно відтворив зміст постанови.

На початку XX ст. *аудит* отримав широке застосування у *фінансовій діяльності*, а в кінці XX ст. його почали застосовувати і в таких областях діяльності людини, як *менеджмент якості* та *екологічний менеджмент*.

Аудит – форма незалежного та нейтрального контролю будь-якої діяльності підприємства, організації, установи, товариства (надалі – *організація*), що широко застосовується у практиці ринкової економіки, особливо у сфері бухгалтерського обліку.

У наш час *спостерігається* ***посилення залежності успішної діяльності організації від функціонування її системи ІБ***. Це пов'язано зі збільшенням об'єму важливих для організації даних, які оброблюються, передаються та зберігаються в її інформаційній системі. А тому, як наслідок, у ТОП-менеджерів організацій зазвичай виникає низка важливих запитань:

– Чи відповідає система ІБ меті та завданням організації, зокрема, розвитку її бізнес-процесів?

– Чи прийнята політика безпеки є адекватною меті та завданням організації, зокрема, розвитку бізнесу?

– Яким чином ефективно контролювати реалізацію виконання політики безпеки в організації?

– Коли необхідно здійснити модернізацію системи безпеки? У який спосіб обґрунтувати необхідність модернізації та пов'язаних з цим видатків?

– Як швидко окупляться інвестиції в ІБ? Як визначити рівень прибутковості/збитковості такого процесу?

– Наскільки правильно виконане конфігурування та налаштування штатних засобів підтримання ІБ організації?

– Як переконатися, що наявні в організації засоби захисту – системи моніторингу та управління ІБ (SIEM), системи запобігання/виявлення витоку конфіденційної інформації (DLP), системи управління мобільними пристроями (MDM), системи захисту віртуальної інфраструктури, міжмережеві екрани (firewall), системи виявлення/запобігання вторгнень (IDS/IPS), антивірусні системи, VPN-шлюзи тощо – ефективно справляються з поставленими перед ними завданнями?

– У який спосіб вирішуються завдання забезпечення конфіденційності, доступності та цілісності інформаційних активів організації?

– Як оцінити роботу підрядних організацій, що виконували проєктування, постачання, запуск та налаштування засобів безпеки? Чи є недоліки, а якщо так, то які?

– Яким чином забезпечити необхідну у практиці роботи організації «вертикаль управління» для централізованого управління її безпекою?

– Як контролювати стан ІБ організації? Які методи та засоби необхідні?

– Що робити після того, як система забезпечення безпеки побудована (є стратегічний та тактичні плани захисту організації, плани роботи при виникненні надзвичайних ситуацій)?

– Чи є необхідність на постійній основі періодично проводити навчання співробітників служби ІБ організації? Якщо так, що який бюджет організації для цього необхідний?

– Яким чином управляти інформаційними ризиками організації? Які інструментальні засоби для цього необхідно задіяти?

– Чи задовольняє стан ІБ організації вимогам міжнародних стандартів оцінювання та управління безпекою, зокрема, стандартів ISO 27001, NIST 800 Series, BSI тощо?

Очевидно, що на усі перелічені запитання (а на практиці їх набагато більше) одразу дати однозначні відповіді неможливо. ***Лише об'єктивний (неупереджений) та незалежний аудит системи менеджменту ІБ дасть достовірну та обґрунтовану відповідь***. Саме такий аудит дає змогу комплексно перевірити всі основні рівні забезпечення ІБ організації: *нормативно-правовий, організаційний, технологічний та апаратно-програмний*.

Аудит інформаційної безпеки є одним із найактуальніших, що швидко розвивається, напрямів стратегічного та оперативного менеджменту в області ІБ та зумовлює постійну зацікавленість з боку фахівців інформаційних технологій. З точки зору загального розвитку організації важливим є *аудит її безпеки*, який включає *аналіз ризиків*, які пов'язані з можливістю здійснення *загроз безпеки*, особливо щодо інформаційних ресурсів, *оцінювання поточного рівня захище-*

ності, *локалізації вузьких місць* у системі захисту, *оцінювання на відповідність нормативно-правовій базі* в області ІБ і *вироблення рекомендацій* із запровадження нових та підвищення ефективності існуючих механізмів безпеки інформаційних систем. Саме для цього і проводиться аудит ІБ.

Отже, можна сформулювати, що ***основне завдання аудиту інформаційної безпеки*** – об'єктивно оцінити поточний стан ІБ організації, а також її адекватність поставленій меті, зокрема, завданням бізнесу для збільшення ефективності та рентабельності економічної діяльності.

Інформаційна безпека – один з видів безпеки, визначається через «*стан захищеності*», що неявно скеровує нас до категорій психології, зокрема, *упевненості та віри у безпеку*. Ця упевненість орієнтована на соціум – людину або групу осіб, що очікують або ж прагнуть досягнути певної мети у результаті своєї діяльності.

У директиві Організації з економічного співробітництва та розвитку [3] щодо безпеки мереж та інформаційних систем зазначено: «*Увесь бізнес побудований на довірі*. *Довіра може розвиватися лише у тому випадку, коли учасники угод відчувають надійність, упевненість та безпеку*».

Наша *упевненість може базуватися лише на знанні* щодо певного об'єкта (системи, процесу – об'єкта довіри), яке отримане або у результаті спостережень, або ж у результаті здійснених заходів як самостійно, так і з залученням інших сторін.

Якщо виходити з передумов, що безпека – це передусім прагнення до порядку (ролі та відповідальності, прав та обов'язків), то, враховуючи невелику кількість існуючих специфічних для безпеки методів (*стандартів*, які стосуються забезпечення безпеки на різних етапах життєвого циклу систем, *процесів*, *продукції*, *довіри* до персоналу тощо), кожний із існуючих методів привносить свою частку в *упевненість у безпеці*. Усе, що може бути використане для створення аргументації для *упевненості у безпеці* та зменшення у цьому зв'язку *невизначеності (ризику*), має надзвичайно важливе значення.

Аудити (*зовнішній/внутрішній*), як і інші напрями оцінювання ІБ, призначені забезпечити підтвердження реалізації заявлених вимог або мети безпеки, що, у свою чергу, скероване на формування *упевненості у безпеці*. А тому важливими є такі запитання:

– Наскільки достовірними (чи їм можна довіряти) є результати аудиту?

– Наскільки результати аудиту є адекватними реальному стану справ?

– Наскільки результати аудиту дозволяють оцінити ступінь досягнення мети ІБ організації та впливу ІБ на бізнес організації?

Перша група запитань пов'язана з якістю методики проведення аудиту, кваліфікацією та досвідом аудиторів, ступенем достовірності наданих у процесі

аудиту свідчень, тобто тими аспектами, які визначають ставлення зацікавленої сторони до результатів аудиту інформаційної безпеки.

Проведення аудиту, як правило, є «ноу-хау» аудиторської організації, аудитора, тобто усе зводиться до *рівня здатності аудиторської організації* до даного виду діяльності (читай – *рівня кваліфікації аудиторів*). Ці аспекти регулюються в усіх сферах аудиторської діяльності або на правовому рівні, або на рівні стандартів.

Друга група запитань пов'язана із забезпеченням повноти перевірки, досліджуваних матеріалів, тобто з програмою аудиту, що у кінцевому результаті дає змогу створити упевненість у досягненні мети аудиту безпеки. Дані обставини також регулюються в усіх сферах аудиторської діяльності або на правовому рівні, або на рівні стандартів.

Третя група запитань пов'язана з принциповою можливістю вирішення за допомогою аудиту проблеми забезпечення прозорості стану захищеності організації від загроз в інформаційній сфері, тобто ІБ, а також її внеску у досягнення головної мети діяльності будь-якої організації. У підсумку – це питання *формування упевненості* у досягненні мети ІБ.

Забезпечення ІБ – це певна сукупність організаційної структури та упорядкованих процесів, у межах якої аудит ІБ є одним із визначальних компонентів. А тому його призначення, процедура проведення, роль тощо повинні розглядатися саме з позиції *забезпечення довіри* до ІБ, а уся відповідна перевірка повинна бути повноцінною системою *забезпечення довіри* до ІБ.

Вимога позитивного оцінювання за результатами аудиту є умовою успішного ведення бізнесу, що засвідчує відповідність організації вимогам визнаного міжнародного стандарту безпеки. Міжнародні стандарти ISO 27001, NIST 800 Series, BSI слугують основою для проведення будь-яких робіт в області ІБ, у тому числі й аудиту безпеки.

На формування та розвиток міжнародних стандартів, які є правовою та методологічною основою аудиту ІБ, безумовно, вплинули законодавчі акти. Серед керівництв з основ аудиту ІБ та власного оцінювання на відповідність ІБ встановленим вимогам (США) є «*Керівництво з аудиту засобів управління федеральних інформаційних систем*» (Federal information system controls audit manual, FISCAM); «*Керівництво власного оцінювання безпеки для систем інформаційних технологій*» (Security Self-Assessment Guide for Information Technology Systems); «*Керівництво з метрик безпеки для систем інформаційних технологій*» (Security Metrics Guide for Information Technology Systems) та інші.

Аудит ІБ, зокрема її інформаційної системи організації, не є одноактним процесом, а його роботи охоплюють низку послідовних етапів:

1. Ініціювання дослідження системи.

2. Збирання інформації.

3. Аналіз отриманих даних.

4. Вироблення рекомендацій.

5. Підготовлення звіту за результатами дослідження.

Можна виділити такі основні ***види аудиту ІБ***:

1. ***Експертний аудит*** безпеки, у процесі якого виявляються недоліки у системі ІБ на основі наявного досвіду експертів, які беруть участь у процесі дослідження системи.

2. ***Оцінювання відповідності*** рекомендаціям міжнародних стандартів, а також вимогам керівних документів.

3. ***Інструментальний аналіз*** захищеності інформаційних систем, скерований на виявлення та усунення вразливостей.

4. ***Комплексний аудит***, який містить усі перелічені форми проведення аудиту.

Залежно від завдань, які необхідно вирішити в організації, кожний з перелічених видів аудиту може проводитися окремо або у комплексі. Об'єктом аудиту може бути як інформаційна система, так і окремі її сегменти, в яких здійснюється оброблення цінної для організації інформації.

Підходи до проведення аудиту безпеки можуть базуватися *на аналізі ризиків*, спиратися на *використання стандартів ІБ* або *поєднувати* ці підходи.

Сучасні методики аналізу ризиків та аудиту ІБ, проєктування та супроводження систем безпеки дають можливість:

– кількісно оцінити поточний рівень безпеки, обґрунтувати допустимі рівні ризиків, розробити план заходів з підтримання необхідного рівня безпеки на організаційно-управлінському, технологічному та технічному рівнях;

– розрахувати та економічно обґрунтувати розмір необхідних фінансових вкладень (інвестицій) у систему безпеки, протиставити видатки на забезпечення безпеки з потенційним збитком та ймовірністю його виникнення;

– виявити та провести першочергові заходи для зменшення найнебезпечніших вразливостей до здійснення нападів на уразливі ресурси;

– визначити функціональні відносини та зони відповідальності при взаємодії підрозділів та осіб, відповідальних за ІБ організації, створити або модифікувати необхідний пакет внутрішніх нормативних документів;

– розробити та узгодити зі службами організації та наглядовими органами проєкт запровадження необхідних комплексів захисту, які враховують сучасний рівень та тенденції розвитку інформаційних технологій;

– організувати підтримання запровадженого комплексу захисту відповідно до умов роботи організації, які постійно змінюються, внутрішніх нормативних документів, модифікацією технологічних процесів та модернізацією технічних засобів захисту.

Вирішення цих та інших важливих проблем функціонування і розвитку організацій завдяки запровадженню інформаційних технологій є неможливим у сучасному суспільстві без запровадження аудиту ІБ організації на регулярній основі.

На основі отриманих результатів аудиту ІБ проводиться підготовка розпорядчих документів, які утворюють основу для проведення захисних заходів («*Концепція інформаційної безпеки*», «*План захисту*», «*Положення про поділ ресурсів інформаційної системи на категорії*» тощо), а також вносяться зміни у посадові інструкції та положення підрозділів організації.

Результати проведення аудиту безпеки організації дають можливість:

1. ***Керівникам організації*** забезпечити:

– формування єдиної політики та концепції безпеки організації; розрахувати, узгодити та обґрунтувати необхідні видатки на ІБ;

– об'єктивно та незалежно оцінити поточний рівень ІБ організації;

– забезпечити необхідний рівень безпеки та у цілому підвищити економічну ефективність організації;

– ефективно створювати та використовувати профілі захисту конкретної організації на основі апробованих та адаптованих якісних та кількісних методик оцінювання ІБ організації замовника.

2. ***Керівникам служб*** ІБ організації:

– отримувати оперативну та об'єктивну оцінку (якісну та кількісну) стану ІБ організації на основних рівнях безпеки: організаційно-технологічному та технічному;

– виробити та обґрунтувати необхідні заходи організаційного характеру (склад, структуру служби ІБ, положення про комерційну таємницю, пакет посадових інструкцій та інструкцій з діяльності у нештатних ситуаціях тощо);

– сформулювати економічне обґрунтування інвестицій у безпеку, обґрунтовано обирати ті або інші апаратно-програмні засоби захисту інформації відповідно до концепції безпеки, а також на основі вимог керівних документів та стандартів;

– адаптувати та використовувати у своїй роботі позитивні кількісні показники оцінювання ІБ, методики оцінювання та управління безпекою з прив'язуванням до економічної складової ефективності організації.

3. ***Системним, мережевим адміністраторам та адміністраторам безпеки*** організації:

– об’єктивно оцінювати безпеку усіх основних компонентів та послуг інформаційної системи організації замовника, технічний стан апаратно-програмних засобів захисту інформації;

– успішно застосовувати на практиці рекомендації, отримані під час виконання аналітичного дослідження, для нейтралізації та локалізації виявлених вразливостей апаратно-програмного рівня.

4. ***Співробітникам організацій***:

– визначити основні функціональні стосунки і, що особливо важливо, зони відповідальності, у тому числі фінансової, за належне використання інформаційних ресурсів та стан політики безпеки організації.

Зазначимо, що нині існує розмаїття як методів аналізу та управління ризиками, так і програмних засобів, які їх реалізують [8–17]. У підручнику ви знайдете їх короткий аналіз.

Узагальнюючи викладене вище, можемо зазначити, що ***запропонований підручник відображає сучасні вимоги***, які висувають до підготовки магістрів за напрямом «Управління інформаційною безпекою» та орієнтований на розгляд методичних та організаційних основ проведення аудиту ІБ.

Запитання для самоконтролю

1. У чому полягає відмінність та особливості проведення зовнішнього та внутрішнього аудиту?
2. Назвіть основні цілі проведення аудиту ІБ.
3. Якою є послідовність дій при проведенні аудиту ІБ в організації?
4. Чим визначаються масштаби аудиту ІБ?
5. З якою метою проводиться аналіз ризиків?