DOI:10.18372/2310-5461.41.13527

УДК 366.56(075.8)

О. К. Юдін, д-р техн. наук, проф.
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0001-5098-7796
e-mail: yak333@ukr.net;

Р. В. Зюбіна, к-т техн. наук
Київський національний університет
імені Тараса Шевченка
orcid.org/0000-0002-8654-6981
e-mail: ziubina@knu.ua;

О. В. Матвійчук-Юдіна, к-т пед. наук
Національний авіаційний університет
orcid.org/ 0000-0002-5906-5023
e-mail: metalen3@ukr.net

СУЧАСНІ ПРАКТИКИ ВПРОВАДЖЕННЯ СИСТЕМИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ

В умовах стрімкого розвитку інфраструктури держави та суспільства, а також поглиблення процесів інформатизації діяльності установ, все більше значення набуває ефективність процесів розробки, впровадження, аудиту, супроводження сучасних інформаційних систем (ІС) та їх безпеки. Сучасне ІТ-середовище об'єктів критичної інфраструктури, а також систем обробки державних інформаційних ресурсів (ДІР), являє собою складну систему, що об'єднує різноманітні інформаційні, нормативні, програмні, технічні, людські й інші види ресурсів з метою якісного досягнення цілей організації, підприємства, установи на ринку послуг. Це зумовлює зростання потреби у підвищенні ефективності використання захищених ІТ та інформаційних систем різних класів, збільшення переваг і усунення недоліків від їх застосування, а також встановлює критерії обґрунтування витрат на забезпечення захищених інформаційно-комунікаційних систем (ІКС; нормативно-правове, організаційне, технічне забезпечення).

Аналіз останніх досліджень і публікацій

Для задоволення вищезазначених потреб все більшого значення набуває регулярне застосування в системі управління організацій системи аудиту та процесів контролю інформаційної безпеки (аудит і контроль ІБ) [1].

Система аудиту і контролю є ключовим компонентом для забезпечення якості функціонування захищених інформаційних систем ї комплексів критичних інфраструктур та ДІР. Без надійних комплексних систем захисту інформації та результативних заходів системи аудиту і контролю, організація не в змозі надійно і якісно виконувати базові процеси надання послуг, забезпечувати процеси захисту інформаційних ресурсів різних класів, виконувати операції/транзакції та узагальнювати надійну діяльність і звітність тощо [2].

Постановка завдання на дослідження

Зміст досліджень полягає у розробці методології, методів та моделей побудови системи аудиту та контролю стану інформаційної безпеки на об'єктах критичної інфраструктури та державних інформаційних ресурсів різник класів.

Мета статті — комплексний підхід до обґрунтування і впровадження системи вітчизняних та міжнародних стандартів, а також нормативно-правових аспектів формування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури та в системах ДІР. Також, метою дослідження повинно бути визначення класифікації методів, моделей і процедур системи аудиту і контролю ІБ, згідно вітчизняних та міжнародних стандартів та вимог.

Вирішення поставленої мети, щодо формування системи аудиту та контролю інформаційної безпеки, повинно бути спрямовано на вирішення фундаментальної проблеми підвищення ефективності організації захисту державних інформаційних ресурсів та критичних інфраструктур в нашій державі.

Ця проблема породжується встановленим протиріччям між:

- наявними зростанням вимог до ефективності і надійності функціонування систем ІБ, а також відсутністю моделей і стандартизованих вимог до проведення процесів аудиту і контролю на об'єктах критичної інфраструктури;
- відсутністю відповідної дієвої методології оцінки ступеня захищеності державних інформаційних ресурсів в країні, терміновою необхідністю внесення змін в законодавчу базу зазначеної сфері.

Слід зазначити, що звертаючись до теми досліджень з захисту ДІР та впровадження системи аудиту і контролю ІБ приділяли увагу, як вітчизняні, так і зарубіжні вчені. Однак, питанню створення системи збору, обробки та аналізу інформації з метою проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури та ДІР приділялась незначна увага, про що свідчить, як існуюча нормативно-правова база, так і взагалі,наявна відсутність на належному рівні система аудиту і контролю стану ІБ автоматизованих систем (АС) в країні. Треба констатувати, що відсутність вітчизняних АС, які б дозволяли здійснювати повноцінну інформаційно-аналітичну діяльність на об'єктах критичної інфраструктури та ДІР, гальмує базові процеси національної безпеки держави [3].

Міжнародний досвід впровадження та забезпечення системи тотального менеджменту якості послуг

Сьогодні майже неможливо уявити організацію, яка б не використовувала інформаційні технології у своїй роботі. Інформація, яка циркулює в компанії може бути як з обмеженим доступом, так і просто містити дані, необхідні для ефективного виконання бізнес-процесів організації. Порушення конфіденційності даних, чи втрата доступу до важливих інформаційних активів може мати негативні наслідки: від неможливості нормального функціонування організації до притягнення до кримінальної відповідальності. Тому, зважаючи на це, підприємство зобов'язане забезпечити захист своєї інформації та її основних властивостей на основі міжнародних стандартів та вимог з урахуванням надання високого рівня якості бізнес послуг.

Система тотального менеджменту якості (англ. Total Quality Management, TQM), це — концепція управління інституцією (підприємством, організацією тощо), яка передбачає загальне цілеспрямоване та ефективно скоординоване застосування технологій, методологій,методів і моделей управління якістю надання бізнес послуг в усіх сферах діяльності сектору індустрії на основі раціонального використання сучасних інформаційних технологій (ІТ).

Міжнародна організація стандартизації (ISO) узагальнила весь накопичений позитивний досвід робіт у сфері підвищення якості продукції і розробила на цій основі стандарти серії ISO 9000 iISO10000, що лягли в основу принципів загального менеджменту TQM.

Стандарти ISO серії 9000 відразу здобули всесвітнє визнання, як особливо популярні документи системи менеджменту. Нагадаємо, що спеціалісти з якості використовують нові стандарти ISO 9000, які враховують зміни, внесені в 2005, 2008 та 2009–2015 роках. Зазначені стандарти, задовольняючи зростаючі потреби споживачів, перетворилися на універсальний інструмент забезпечення, оцінювання і контролю систем якості підприємства [4].

Зазначені стандарти містять перевірені часом концепції та моделі не лише внутрішнього, а й зовнішнього принципу управління якістю продукції та послуг, встановлюють зворотній зв'язок : підприємство — споживач.

Сучасна система TQM впроваджена з метою досягнення довгострокового успіху підприємства на базі максимального задоволення ринку послуг і користувачів.

Завданнями TQM є постійне поліпшення якості бізнес процесів,шляхом системного аналізу (аудиту і контролю) результатів та коригувальних дій організації для забезпечення конкурентоспроможності за рахунок використання передових технологій, а також гнучкості, своєчасних поставок послуг та продукції, безперервне вдосконалення якості продукції та процесів, використання наукових підходів до вирішення задач промисловості, синергії персоналу від керівників організації до користувачів продукції [5].

Система менеджменту інформаційної безпеки (СМІБ, англ. Information Security Management System, ISMS) є частиною загальної системи менеджменту підприємства та створена для вдосконалення стану інформаційної безпеки.

Система має «процесінговий» та«ризикорієнтований» підхід, що означає, що головною ідеєю та головним завданням СМІБ є процеси аналізу та управління інформаційними ризиками при створенні, впровадженні, функціонуванні, моніторингу та підтримці стану захищеності інформаційних ресурсів компанії.

Актуальність створення СМІБ пояснюється тим, що зараз відбувається загальна інформатизація суспільства і все більше установ впроваджують у свою діяльність використання інформаційних технологій для обробки даних.

Зі зростанням кількості міжнародних стандартів та рекомендацій до створення СМІБ, все більше організацій намагається впровадити таку систему і у себе на підприємстві. Рішення зі створення СМІБ приймається вищим керівництвом, яке в подальшому ініціює створення групи по її плануванню, супроводженню та контролю.

Відповідальність за впровадження та супровід СМІБ покладається на відповідний орган або окремих спеціалістів — інспекторів. Однак, лише за умови участі в цьому процесі вищого керівництва та персоналу компанії функціонування СМІБ матиме позитивні результати [6].

Загалом, побудова СМІБ передбачає впровадження взаємозалежних процесів відповідно до вимог міжнародних стандартів в сфері ІБ, в яких виділяють такі основні процеси: управління інформаційними активами організації;управління ризиками інформаційної безпеки;управління інцидентами;управління персоналом та навчання;розробка та впровадження документації в області забезпечення інформаційної безпеки; управління процесами забезпечення та змін конфігурації ІКС;контроль дотримання вимог інформаційної безпеки;моніторинг ефективності процесів інформаційної безпеки.

СМІБ на об'єктах критичної інфраструктури та ДІР дозволяє «об'єднати» всі процеси забезпечення ІБ та чітко визначити взаємозв'язок бізнес-процесів, відповідальних осіб, ресурси, які необхідні для їх ефективного функціонування.

Для ефективної роботи СМІБ не менш важливим є те, що необхідно враховувати всі особливості об'єкту, на якому планується впровадження СМІБ: величину організації, її сферу діяльності, бізнес-потреби, інформаційні активи, інформаційні потоки, які в ній циркулюють та їх рівень критичності.

Впровадження процесів управління ІБ відбувається шляхом створення необхідної документації, яка буде регламентувати ці процеси, визначати відповідальних за них осіб, їх посадові інструкції, як для керівництва установи, так і для всього персоналу.

Аудит та оцінка якості ІТ послуг в сфері інформаційної безпеки.

Аудит систем управління інформаційною безпекою на об'єктах критичної інфраструктури та ДІР, є не менш важливою складовою діяльності підприємства та забезпечення його інформаційної безпеки. Для ефективної роботи СМІБ необхідно постійно перевіряти її результативність, здатність протидії встановлених методів і засобів загрозам. Зрозуміло, що результатом проведення системи аудиту, моніторингу та контролю стану ІБ, обов'язково повинні бути впровадженні процеси добору забезпечень з метою протидії або профілактики виявлених недоліків, а також процедури ліквідації наслідків і поновлення бізнес процесів. За відсутності регулярного аудиту, підприємство може вчасно не помітити зростання новостворених ризиків або збоїв в роботі СМІБ та понести небажані втрати, навіть з урахуванням великої вартості використаної інформаційної системи.

Щорічно міжнародні організації, такі як: ISO, IEC, ITU-T, ONZ, а також Громадські об'єднання ISACA, IETF, CISA, $(ISC)^2$, удосконалюють способи та процедури проведення аудитів, підвищують міру відповідальності за невідповідність міжнародним чи національним вимогам стандартів та встановлюють обов'язковість уведення процедур проведення внутрішніх та зовнішніх аудитів, моніторингу, процедур контролю ефективності ІБ. Власники організацій сприймають цей факт досить неоднозначно, оскільки розробка, побудова, впровадження СМІБ та проведення її моніторингу є досить затратним та ресурсномістким процесом. Крім того, створення СМІБ на об'єктах критичної інфраструктури та ДІР не дає наявного прибутку, а отже показник повернення таких інвестицій є непомітним.

Питання інформаційної безпеки на об'єктах критичної інфраструктури та ДІР, є одним з найбільш актуальних та, відповідно, складних завдань, що стоять перед компаніями. Керівники та працівники, що відповідальні за внутрішній аудит системи управління інформаційною безпекою, або незалежні аудитори (сторонні фахівці) відіграють важливу роль у впровадженні та забезпеченні реалізації питань стосовно необхідності створення СУІБ та проведення її регулярного моніторингу.

Необхідно розуміти, що створення СУІБ є важливим етапом для досягнення ефективної роботи будь-якої організації, функціонування якої так чи інакше залежить від ІТ та працездатності її інформаційних систем. Аудит інформаційної безпеки, в свою чергу, є ключем, фундаментом, що підкреслює важливість ефективного впровадження стратегії інформаційної безпеки на підприємстві та дозволяє виявити існуючі недоліки в захисті інформаційних активів компанії.

Аналіз міжнародних стандартів та практик в області інформаційної безпеки

На сьогодні існує велика кількість нормативно-правових документів, які регламентують процеси створення, впровадження, перевірки та вдосконалення СМІБ на об'єктах критичної інфра-

структури та ДІР, тому підприємства, які прагнуть отримати високий рівень гарантій якості та ефективності захисту своїх інформаційних активів, користуються вже розробленими в цій області світовими практиками.

Стандарти з управління безпекою інформаційних технологій створюються на основі аналізу та узагальнення кращих методик, ефективність яких вже була підтверджена ІТ-спеціалістами та досвідом на ринку послуг великої кількості організацій.

Класифікацію стандартів в галузі інформаційної безпеки на об'єктах критичної інфраструктури та ДІР можна провести за напрямами: залежно від масштабів впровадження і визнання (у т.ч. географічному) та залежно від виникнення або джерела формування і визнання: стандарти «де-юре» та «де-факто».

У першому випадку стандарти поділяють на міжнародні, національні, галузеві — «де-юре». В другому випадку існують так звані стандарти: «де-факто», які діють всередині конкретної корпорації, Громадського об'єднання, асоціації промисловців ринку послуг тощо.

«Де-юре» стандарти створюються загально визнаними офіційними організаціями, які спеціалізуються на стандартизації. «Де-факто» означає, що стандарт було створено певною компанією або громадськими організаціями для потреб, строго визначеного за напрямами, ринку промисловості.

Ураховуючи офіційність стандартів «де-юре» та обов'язковість дотримання їх вимог в тій чи іншій регіональній зоні, більшість організацій при створенні СМІБ зазвичай використовують рекомендації стандартів «де-факто», вважаючи їх більш повними, ефективними, зрозумілішими та найголовніше адаптованими до сектору індустрії конкретизованої галузі.

Прикладом об'єднання напрямів та стандартизації застосування інформаційно-комунікаційних систем та надання високого рівня якості послуг в ІТ галузі, призвело до об'єднання двох міжнародних організацій — Міжнародної електротехнічної комісії (IEC) та Міжнародної організації зі стандартизації (ISO), що зумовило створення об'єднаного підрозділу Joint Technical Committee. Комітет займається питаннями, пов'язаними з розробкою та вдосконаленням міжнародних стандартів «де-юре» в області інформаційних технологій.

Стандарти, які стосуються безпосередньо управління інформаційною безпекою являють собою сімейство стандартів ISO/IEC 270xx та слугують основним нормативним документом при побудові СМІБ та аудиті ІБ.

Українськими аналогами стандартів «де-юре» на рівні нашої країни виступають Державні технічні стандарти України (ДСТУ), частина з яких є перекладом та адаптацією міжнародних та європейських стандартів, прийнятих зі змінами або без.

Аудит та контроль рівня СМІБ, як складова загального менеджменту підприємства, проводиться для перевірки відповідності вимогам світових та вітчизняних стандартів та з метою забезпечення безперервності бізнес процесів на основі управління ризиками. Підґрунтям цих процесів, зрозуміло, повинна бути нормативно-правова база, яку можна класифікувати за напрямами:система стандартів з тотального менеджменту якості TQMISO 9000\90xx, ISO 10000\100xx; нормативно-правові документи країни в галузі інформаційної безпеки (для нашої держави — закони України, ДСТТУ, НД ТЗІ, НД КЗІ тощо); міжнародні стандарти серії ISO/IEC; міжнародні компаративні стандарти Громадських об'єднань та асоціацій ISACA, IETF, CISA, $(ISC)^2$, ITIL, PRINCE2, COBIT5, PCI DSS.

Необхідність проведення регулярного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та ДІР полягає в здійсненні оцінки реального стану захищеності ресурсів інформаційних (ІС) та їх спроможності протистояти зовнішнім і внутрішнім загрозам інформаційної безпеки, які постійно змінюються та адаптуються до сучасного інформаційного середовища і вдосконалюються технічно. Аудит інформаційної безпеки на об'єктах інформаційної діяльності проводиться з метою визначення стану захищеності його ІС, засобами якої обробляється конфіденційна чи інша критична інформація замовника, а також відповідності ІС на об'єктах критичної інфраструктури стандартам та нормативним документам в державному, комерційному та банківському секторі.

Крім цих «загальних» стандартів, існує ще ціла низка міжнародних документів, що регламентують діяльність компаній в певній сфері. Так, для організацій, що працюють в платіжними системами, важливим є наявність сертифікації на відповідність вимогам стандарту PCI DSS (Payment Card Industry Data Security Standard) — стандарт безпеки даних індустрії платіжних карт, розроблений міжнародними платіжними системами Visa та Master Card. Будь-яка організація, що приймає та обробляє дані банківських карт (як онлайн, так і офлайн) повинна відповідати вимогам PCI DSS. У випадку з цим міжнародним документом, існує чотири рівні сертифікатів залежно від максимальної кількості оброблюваних стандартів.

Не секрет, що кожна країна має свої політичні та національні особливості формування об'єктів критичної інфраструктури, тому наразі ще не існує загальноприйнятого стандарту «де-факто», який би задовольняв потреби всіх країн та організацій в галузі ІТ та їх безпеки, без виключення. Стандарти «де-юре», в більшості випадків, є досить узагальненими та несуть рекомендаційний характер. Зважаючи на цей факт, не дивним є створення та існування великої кількості стандартів та нормативних документів, що супроводжують або більш детально розкривають базові стандарти та конкретизують їх за вимогами або галуззю. Яскравим прикладом таких стандартів можуть бути — національні (ANSI, SCC, NIST, USA, BSI, ДСТУ — Україна, або польська — PKN) або т. звані «крайові» в області управління та безпеки інформаційних технологій, які є більш детальними, та які мають більш практичні рекомендації і поради.

На даний час, в Україні, офіційно прийняті такі стандарти з серії ISO/IEC 27K, як: ДСТУ ISO/IEC 27000, в якому описуються основні поняття та визначення; ДСТУ ISO/IEC 27001:2015, що слугує основним стандартом при побудові і супроводі СМІБ та у якому визначені основні вимоги до інформаційної системи і її безпеки; ДСТУ ISO/IEC 27002:2015, який містить більш детальні вимоги, рекомендації та опис процесів управління інформаційною безпекою;ДСТУ ISO/IEC 27005:2015 в якому описуються основні підходи по управління ризиками та забезпеченнями;ДСТУ ISO/IEC 27006:2015, який визначає перелік вимог до органів, які здійснюють аудит та сертифікацію системи СМІБ; ДСТУ ISO/IEC 15408 -1...3, у яких зазначені критерії оцінювання та забезпечення рівня гарантій системи безпеки підприємства. В Україні прийнято всі 3 частини стандарту ISO/IEC 15408 та опубліковано в якості ДСТУ, позначення й найменування відповідного стандартів серії:

- ДСТУ ISO / IEC 15408-1: ISO/IEC 15408-1-20XX «Інформаційна технологія. Методи й засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 1. Введення й загальна модель».
- ДСТУ ISO / IEC 15408-2: ISO/IEC 15408-2-20XX «Інформаційна технологія. Методи й засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 2. Функціональні компоненти безпеки».
- ДСТУ ISO / IEC 15408-3: ISO/IEC15408-3-20XX «Інформаційна технологія. Методи й засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 3. Компоненти Довіри».

Цікавий той факт, що в Україні з'явилась низька стандартів з організації центрів аудиту та підготовки і атестації аудиторів з ІБ, які регламентують порядок проведення аудиту та контролю інформаційної безпеки в рамках системи тотального менеджменту підприємства, а саме:

- ДСТУ ISO/IEC 27006:2015, «Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою»;
- ДСТУISO / IEC 17021 «Оцінка відповідності. Вимоги згідно ISO/IEC 17021-1:2015 до органів, що здійснюють аудит і сертифікацію систем менеджменту».

Документ розроблено і впроваджено в 2016 р. Національним агентством з акредитації України (далі — НААУ) відповідно до Політики НААУ щодо застосування вимог міжнародних стандартів під час акредитації (ЗД-08.00.11). Документ опрацьовано спільно з Технічним комітетом з акредитації. Цей документ є неофіційним перекладом та носить інформаційний характер, при цьому рекомендується використовувати стандарт 17021-1:2015 на англійській мові. Документ рекомендований для використання органами з оцінки відповідності, персоналом з акредитації, працівниками НААУ, іншими зацікавленими сторонами.

Стандарт ISO/IEC 17021 містить принципи та вимоги до компетентності, послідовності та неупередженості органів, що провадять аудит та сертифікацію всіх типів систем менеджменту.

Важливим є той факт, що органи з сертифікації, що діють відповідно до цієї частини ISO/IEC 17021 не мають необхідності пропонувати сертифікацію систем менеджменту всіх типів. Інші типи і класи стандартів можуть бути запропоновані організацією на розсуд власних потреб згідно складових ринку послуг та нормативно-правових вимог країни.

- ISO/IEC 17024 «Схема сертифікації персоналу. Експерт з оцінки відповідності у сфері дії технічних регламентів пс.01.2015».

В стандарті встановлюються вимоги і рекомендації до сертифікації експертів з оцінки відповідності у сфері дії технічних регламентів. Необхідна компетентність визначається специфічними вимогами окремого регламенту, відповідно до п. 8.2. ДСТУ EN ISO/IEC 17024:2014. Компетентність екзаменаційної комісії забезпечується участю експертів та фахівців належного рівня, які мають необхідний рівень знань у сфері дії окремого технічного регламенту (відповідно до п. 6.2.2.1. ДСТУ EN ISO/IEC 17024:2014).

Це свідчить про то що, впроваджено ще один крок нашого суспільства до розуміння важливос-

ті місця системи аудиту в загальній системі тотального менеджменту.

Така різноманітність стандартів у сфері управління інформаційними технологіями та інформаційною безпекою надає організаціям змогу обрати саме ту методику, той підхід, який найкращим чином підійде до особливостей бізнес процесів і ринку послуг. Практика сучасного менеджменту в галузі ІБ передбачає комплексний підхід до формування СМІБ на підприємстві, а також до практик проведення внутрішнього і зовнішнього аудиту, ґрунтуючись на певному, найбільш ефективному для організації, комбінованому переліку нормативних стандартів та вимог.

Аналіз міжнародних стандартів та практик в області аудиту та контролю стану інформаційної безпеки

Аудит інформаційної безпеки на об'єктах критичної інфраструктури є системним процесом одержання комплексної оцінки рівня інформаційної безпеки, а також об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційно-комунікаційних систем (або інформаційно-телекомунікаційної системи) з урахуванням основних факторів: персоналу, процесів та технологій, для подальшого створення СУІБ або перевірки ефективності роботи вже створеної системи менеджменту.

Європейський підхід до системи аудиту, ґрунтується на порівняльному аналізі поточного стану інформаційної системи та забезпеченні бажаного рівня її ефективності. В нашій країні,визначається за підсумками аналізу та контролю системи менеджменту інформаційної безпеки підприємства за моделлю вимог стандартів ISO 27001\ISO 270xx та комплексу ДСТУ ISO/IEC.

Сучасна практика визначає аудит, як технічну складову загального менеджменту ІБ та характеризує його, як контроль та перевірка матеріально-технічних ресурсів організації, інформаційних систем (або автоматизованих, АС) об'єктів критичної інфраструктури та ДІР, зокрема компонентів інформаційно-комунікаційних систем та мереж, систем безпеки на предмет їх відповідності встановленим вимогам та встановленій політиці ІБ.

Основними завданнями аудиту на об'єктах критичної інфраструктури та ДІР є: оцінка поточного стану інформаційної безпеки; ідентифікація та ліквідація уразливостей; мінімізація збитків від потенційних або реалізованих загроз; перевірка СМІБ на відповідність національним та міжнародним стандартам і нормативним документам, надання ефективних рекомендацій до зниження ризиків та підвищення рівня ІБ.

Однак, найголовніше, процедури внутрішнього та зовнішнього аудиту аналізують динаміку стану захисту інформації на підприємстві, формалізують її звітність та допомагають вищому керівництву зрозуміти та отримати впевнитись в тому, що цілі політики інформаційної безпеки лежать в одній площині з бізнес цілями і бізнес процесами компанії.

Світова практика показує, що все частіше для вирішення більшої частини напрямів ІБ підприємства, які виникають при розробці, впроваджені та експлуатації інформаційних систем, використовується термін «технічний менеджмент» та «технічний аудит інформаційних систем» [7].

Аудит та контроль якості ІБ на об'єктах критичної інфраструктури та ДІР повинен забезпечувати виконання наступних базових функцій «технічного менеджменту»: інвентаризацію й розширену діагностику ресурсів ІКС та їх мереж; постійний контроль функціонування мережного устаткування, прикладних систем і мережних сервісів; збір статистики й візуалізацію ключових показників продуктивності й операційних параметрів мережної інфраструктури; оптимізацію навантаження на мережне устаткування й сервери; фіксацію інцидентів та характеристик не санкціонованого впливу різного походження; динамічний аналіз впливу ризиків на бізнес-процеси, і критично важливі додатки;локалізацію причин інциденту і його автоматичне усунення;автоматизований звіт та документування інформаційних потоків впровадженої системи аудиту і контролю стану ІБ; контроль за дотриманням вимог до відповідальних осіб, тощо.

Використання подібних практик з методики технічного менеджменту, дозволяє організації здійснювати моніторинг забезпечення, доступності, стану й продуктивності компонентів на об'єктах критичної інфраструктури, аналізувати й оптимізувати навантаження комунікаційних вузлів, а також прогнозувати виникнення позаштатних ситуацій тощо. Наприклад, менеджмент ризиків може здійснюватися на основі методів CORAS, CRAMM, Magerit, Mehari, Octave та інших.

Аналіз ризиків має доповнюватися процедурами аудиту, який сприяє глибшому розумінню бізнес-процесів, які опановані в організації.

Найвідоміші стандарти та відповідні їм методології, моделі та практики побудови системи менеджменту та аудиту ІБ на об'єктах критичної інфраструктури Серія ISO, CoBiT, CRAMM,ITIL, CORAS.

На практиці, частіше за все зустрічається поєднання ITIL та COBIT. Крім того, COBIT

досить добре та ефективно поєднується з ISO/IEC 270xx, що фокусується на питаннях безпеки. COBIT, у свою чергу, орієнтується на потреби вищого рівня підприємства — покращення загальних бізнес-процесів та досягнення бізнес-цілей за допомогою контролю управління інформаційними технологіями.

COBIT є стандартом управління та аудиту IT; ITIL містить рекомендації до управління IT — послугами. Але при цьому ITIL є бібліотекою кращого практичного досвіду в галузі надання IT-послуг, а COBIT має більш широке призначення — він спеціалізується як на управлінні, так і на аудиті IT.

Висновки

Розроблено основні концептуальні підходи до проведення процедур забезпечення аудиту та контролю системи ризиків, а також ефективності функціонування комплексів інформаційної безпеки на об'єктах критичних інфраструктур. Показано сучасні критерії оцінки якості, як сукупності вимог оцінювання ефективності функцій захисту інформації; наведено методи та моделі оцінювання ефективності функцій захисту інформації, а також форму подання результатів забезпечення процесів аудиту і контролю системи ІБ; визначено методології побудови системи обробки та аналізу інформації з аудиту інформаційної безпеки на об'єктах критичної інфраструктури та в системах обробки ДІР.

ЛІТЕРАТУРА

1. **Юдін О. К.**, Бучик С. С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології*. 2013. Т. 19. № 3. С. 299–304.

2. **Юдін О. К.**, Бучик С. С. Аналіз загроз державним інформаційним ресурсам. *Проблеми інформатизації та управління*. 2013. Т. 4. №. 44. С. 93–99.

3. **Юдін О. К.**, Бучик С. С. Правові аспекти формування системи державних інформаційних ресурсів. *Безпека інформації*. 2014. Т. 20. № 1. С. 76–82.

4. **ISO I**. IEC 27001Information technology, securityte chniques, information security management systems requirements. ISO, Geneva. 2005.

5. **Бекетнова Ю.**, Крылов Г., Ларионова С. Международные основы и стандарты информационной безопасности финансово-экономических систем. Litres, 2018.

6. **Макаренко С. И.** Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий. *Системы управления, связи и безопасности*. 2018. № 1. Методологія управління інформаційними технологіями [Електронний ресурс] URL: https://it60.webnode.com.ua. (дата звернення 20.12.2018)

7. **Якименко Ю. М.,** Наконечний В. С., Толюпа С. В. Оцінка захищеності інформації в автоматизованих інформаційних системах за допомогою загальних критеріїв. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2015. №6 (40). С. 27–31.

8. **COBIT**. [Електронний ресурс] URL: https://en.wikipedia.org/wiki/COBIT. (дата звернення 20.01.2018).

9. **Томас Сигерс**. ITIL: «за» и «против». 10 способов полюбить ITIL еще сильнее. *itSFM*. 2014. №1. С.4–14.

Юдін О. К., Зюбіна Р. В., Матвійчук-Юдіна О. В.

СУЧАСНІ ПРАКТИКИ ВПРОВАДЖЕННЯ СИСТЕМИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Представлено комплексний підхід до обґрунтування і впровадження системи вітчизняних та міжнародних стандартів, а також нормативно-правових аспектів формування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури та в системах державних інформаційних ресурсів. Визначено, що система менеджменту інформаційної безпеки є частиною загальної системи менеджменту підприємства та створена для вдосконалення стану інформаційної безпеки.

Система має «процесінговий» та «ризик-орієнтований» підхід, що означає, що головною ідеєю та головним завданням СМІБ є процеси аналізу та управління інформаційними ризиками при створенні, впровадженні, функціонуванні, моніторингу та підтримці стану захищеності інформаційних ресурсів компанії. Європейський підхід до системи аудиту, ґрунтується на порівняльному аналізі поточного стану інформаційної системи та забезпеченні бажаного рівня її ефективності. В нашій країні, визначається за підсумками аналізу та контролю системи менеджменту інформаційної безпеки підприємства за моделлю вимог стандартів ISO 27001\ISO 270xx та комплексу ДСТУ ISO/IEC.

Таким чином, різноманітність стандартів у сфері управління інформаційними технологіями та інформаційною безпекою надає організаціям змогу обрати саме ту методику, той підхід, який найкращим чином підходить до особливостей бізнес процесів і ринку послуг. Показано сучасні критерії оцінки якості, як сукупності вимог оцінювання ефективності функцій захисту інформації; наведено методи та моделі оцінювання ефективності функцій захисту інформації, а також форму подання результатів забезпечення процесів аудиту і кон-

тролю системи ІБ; визначено методології побудови системи обробки та аналізу інформації з аудиту інформаційної безпеки на об'єктах критичної інфраструктури та в системах обробки ДІР.

Ключові слова: система менеджменту інформаційної безпеки; державні інформаційні ресурси; стандарт; аудит системи; система обробки інформації.

Yudin O., Ziubina R., Matviichuk-Yudina O.

THE MODERN PRACTICES OF IMPLEMENTATION OF THE INFORMATION SECURITY AUDIT SYSTEM ON THE CRITICAL INFRASTRUCTURE OBJECTS

An integrated approach to the justification and implementation of the system of domestic and international standards, as well as regulatory and legal aspects of the formation of the information security audit system at critical infrastructure facilities and in the systems of state information resources is presented. It is determined that the information security management system is part of the overall management system of the enterprise and is designed to improve the state of information security. System "processing" and "risk-oriented" approach, which means that the main idea and the main task of the information security management system are the processes of analysis and management of information risks in the creation, implementation, operation, monitoring and support of the state of security of information resources of the company. The European approach to the audit system is based on a comparative analysis of the current state of the information system and ensuring the desired level of its effectiveness. In our country, is determined by the analysis and control of the information security management system of the enterprise on the model requirements of ISO 27001 \ ISO 270xx and a set of state standards of Ukraine ISO / IEC. Thus, a variety of standards in the field of information technology and information security management provides organizations with the opportunity to choose the methodology, the approach that best suits the features of business processes and the service market. Current criteria of quality assessment, as a set of requirements assessment of the effectiveness of the security features information; the methods and models of assessing the effectiveness of security features information as well as the presentation of the results of the processes of audit and control of information security are defined the methodology of the system of processing and analysis of information audit of information security in the critical infrastructure and treatment systems of the state information resources.

Keywords: Information Security Management System; government information resources; standard; system's audit; information processing system.

Юдин А. К., Зюбина Р. В., Матвийчук-Юдина Е. В.

СОВРЕМЕННЫЕ ПРАКТИКИ ВНЕДРЕНИЯ СИСТЕМЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Представлен комплексный подход к обоснованию и внедрению системы отечественных и международных стандартов, а также нормативно-правовых аспектов формирования системы аудита информационной безопасности на объектах критической инфраструктуры и в системах государственных информационных ресурсов. Определено, что система менеджмента информационной безопасности является частью общей системы менеджмента предприятия и создана для совершенствования состояния информационной безопасности. Система «процессинговый» и «риск-ориентированный» подход, что означает, что главной идеей и главной задачей СМИБ являются процессы анализа и управления информационными рисками при создании, внедрении, функционировании, мониторинге и поддержке состояния защищенности информационных ресурсов компании. Европейский подход к системе аудита, основывается на сравнительном анализе текущего состояния информационной системы и обеспечении желаемого уровня ее эффективности. В нашей стране, определяется по итогам анализа и контроля системы менеджмента информационной безопасности предприятия по модели требований стандартов ISO 27001 \ ISO 270xx и комплекса ГОСТУ ISO / IEC. Таким образом, разнообразие стандартов в области управления информационными технологиями и информационной безопасностью предоставляет организациям возможность выбрать именно ту методику, тот подход, который наилучшим образом подходит к особенностям бизнес процессов и рынка услуг. Показано современные критерии оценки качества, как совокупности требований оценки эффективности функций защиты информации; приведены методы и модели оценки эффективности функций защиты информации, а также форму представления результатов обеспечения процессов аудита и контроля системы ИБ, определено методологии построения системы обработки и анализа информации по аудиту информационной безопасности на объектах критической инфраструктуры и в системах обработки ГИР.

Ключевые слова: система менеджмента информационной безопасности; государственные информационные ресурсы; стандарт; аудит системы; система обработки информации.

Стаття надійшла до редакції 21.02.2019 р.
Прийнято до друку 05.03.2019 р.