Пліс Геннадій Володимирович,
к.т.н, Голова Державної аудиторської служби України, м. Київ
ORCID 0000-0003-2560-6036;

Котух Євген Володимирович,
к.т.н, доцент кафедри комп'ютерних наук,
Сумський державний університет, м. Суми
ORCID 0000-0003-4997-620X;

Нехороших Дмитро Михайлович,
аудитор компанії Legal Strategy Advisors, м. Київ
ORCID 0000-0002-6455-2221;

Халімов Геннадій Зайдулович,
д.т.н., проф., завідувач кафедри безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки, м. Харків
ORCID 0000-0002-2054-9186;

Кучма Ольга Миколаївна,
начальник Управління нормативно-методологічного забезпечення процесу державного фінансового контролю, Державна аудиторська служба України, м. Київ
ORCID 0000-0002-7983-7545

УДК 351.865 **doi: 10.34213/db.21.01.06**

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК НЕОБХІДНА СКЛАДОВА УПРАВЛІННЯ В ДЕРЖАВНИХ УСТАНОВАХ

У статті проаналізовано поточний стан забезпечення аудиту у сфері кібербезпеки в державних установах, визначено типи аудиту, цілі та результати. В статті подано аналіз аудиту інформаційної безпеки як явища, наведені його основні види та характеристики, проаналізовані основні напрямки, методики, програмні інструменти за допомогою яких проводиться експертний та сертифікаційний аудит. Запропоновано подальші кроки для впровадження стратегії кібераудиту та розробки ефективних моделей реалізації кібераудиту, як необхідної складової управління.

Ключові слова: кібербезпека; кібераудит; кібератака; державні установи; врядування.

Постановка проблеми. Сьогодні інформаційні системи (ІС) відіграють ключову роль у забезпеченні ефективності роботи державних установ, підприємств, організацій (далі – установи). Державні установи використовують різноманітні ІС для зберігання, обробки та передачі інформації. Зазначене актуалізує проблеми захисту інформації, що накопичується, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що призводять до значних державних фінансових і матеріальних втрат.

Будь-яка установа, що планує стратегію безперервного існування та функціонування для досягнення своїх цілей, незалежно від правової та організаційної форми господарювання повинна розуміти та усвідомлювати необхідність захищати одну з основ своєї діяльності – інформацію, яка є найціннішим активом установи, та автоматизовані інформаційно-комунікаційні системи як невід'ємну частину цього активу.

Державні установи більшою мірою пов'язані з критичними сферами життєдіяльності держави, органів державної влади, зокрема судової, законодавчої та виконавчої, найважливішими секторами економіки, такими як охорона здоров'я, транспорт, енергетика, адміністративний апарат тощо. Для ефективного захисту інформації установам необхідна об'єктивна оцінка рівня безпеки інформаційних систем та їх постійне удосконалення. Саме для цих цілей і застосовується ***аудит інформаційної безпеки*** або ***кібераудит***.

Здійснення будь-якої діяльності в сучасних умовах, яка відзначається високим рівнем турбулентності, структурними трансформаціями та виникненням нових некерованих факторів впливу, зокрема пандемія COVID-19, висуває підвищені вимоги до своєчасності, достовірності, повноти та якості інформації, що має бути пристосована до запитів користувачів.

Уже на початку цього року відбулися потужні сплески кібератак по всьому світу, в тому числі в Україні. Тільки в перший тиждень січня 2021 р. було зафіксовано 16 хакерських атак на сайти Національного антикорупційного бюро України та Державної служби спеціального зв'язку та захисту інформації України. Через дії хакерів Пакистан з 200 мільйонним населенням був повністю позбавлений електричної енергії майже на добу. Російські хакери змогли

скористатися інструментом, розробленим JetBrains, який базується в Чехії, для отримання доступу до інформації систем федеральних урядів та приватного сектору в США. Німецькі правоохоронні органи закрили Інтернет-майданчик, де користувачі купували та продавали наркотики, викрадали дані та хакерські засоби. Форум, відомий як DarkMarket, був найбільшим в Інтернеті ринком незаконних товарів, повідомило Європейське поліцейське агентство Європол, в якому було задіяно понад 2400 продавців та проведено 320000 транзакцій.

Аналіз інформаційних ресурсів демонструє трансформації моделей атак та моделей поведінки кіберпорушників як змінюються пріоритети в об'єктах атак, каналах витоку інформації. У кіберпорушників з'являються нові програмні та апаратні комплекси, які дозволяють скоювати більш складні й потужні атаки, організація яких не потребує високої кваліфікації та рівня інтелектуальної підготовки.

Зазначене змінює підхід до всієї системи безпеки інформації. Світові практики аудиту інформаційної безпеки показали, що замало побудови інформаційної системи установи за певними стандартами безпеки. Інформаційна безпека будь-якої установи повинна знаходитися в системі активного аудиту, одним із інструментів якого є критичне тестування інформаційних систем та моделювання реальних та актуальних для атак та загроз. А відтак, інформаційна система будь-якої установи повинна бути побудована у відповідності з актуальними світовими стандартами щодо інформаційної безпеки, повинна бути сертифікована та перебувати у стані постійної підтримки відповідності цим стандартам. Виникає логічна потреба у застосуванні технологій задля забезпечення безперервності діяльності державних установ, які задіяні в критично важливих процесах функціонування держави, а тому потребують максимальної уваги до інформаційної безпеки. Вважаємо, що саме система аудиту наразі є фундаментом для формування відносно безпечного інформаційного середовища, через його здатність до кваліфікованої та високоінтелектуальної обробки великих масивів даних установ, мінімізації рівня інформаційної асиметрії.

Враховуючи, що наразі практично вся інформація будь-якої установи сконцентрована в мережі електронних облікових систем, ресурси яких дозволяють підвищити ефективність статутної діяльності, а використання

інформаційних технологій має високий ступінь ризику внутрішнього і зовнішнього втручання в інформаційну архітектуру (нерегламентований внутрішній доступ, відсутність збереження протоколу дій користувача у системі, зовнішнє втручання, зараження вірусами тощо), зумовлюється збільшення фінансових та матеріальних витрат через необхідність постійного забезпечення відповідності стану ІТ-складової установи стратегічним цілям та зовнішньому середовищу.

Саме тому актуалізується вирішення проблеми розвитку аудиту інформаційних систем у світі, удосконалення світових стандартів та впровадження сертифікації, застосування різних методів та прийомів, а також програмних засобів для проведення аудиту інформаційної безпеки у галузях економіки та державному управлінні.

Аналіз останніх досліджень і публікацій. Проблемам аудиту інформаційної безпеки присвячено роботи В. Аверченкова, А. Астахова, С. Петренка. Питаннями правового забезпечення аудиту інформаційної безпеки опікуються О. Синакова та О. Бакалінский. Проте засади практичної розбудови ефективної системи кібераудиту як складової управління органів влади та державних підприємств залишається поза увагою науковців.

Мета статті – аналіз аудиту як головного та базисного елемента інформаційної безпеки будь-якої установи, визначення його ролі в ІТ-сфері та у сфері безпеки інформації, представлення бачення моделі системи аудиту інформаційної безпеки державної установи, визначення її ключових елементів. Об’єктом дослідження є аудит інформаційної безпеки установ.

Викладення основного матеріалу. Потенціал аудиту включає аудит інформаційних систем, які, на нашу думку, є головним і єдиним інструментом перевірки використовуваних установою інформаційних систем, систем безпеки, систем зв’язку з зовнішнім середовищем, корпоративної мережі на предмет їх відповідності бізнес-процесам компанії, а також відповідності міжнародним стандартам, з подальшою оцінкою ризиків збоїв в їх функціонуванні. В сучасних умовах, коли інформаційні системи пронизують усі сфери діяльності, а з урахуванням необхідності їх зв’язку з Інтернет вони виявляються відкритими

для реалізації зовнішніх і внутрішніх загроз, проблема інформаційної безпеки стає не менш важливою, ніж фізична або економічна безпека.

Поняття аудиту виникло з розвитком економіки як науки та з початком активного впровадження системи управління (менеджменту) як у цілому, так і в окремих його складових [1]. Існує декілька ключових визначень аудиту, в яких розкривається його суть як інструменту управління установою.

Аудит (audit) – це систематичний, незалежний і задокументований процес для отримання об'єктивного свідчення і об'єктивної оцінки щодо ступеня досягнення визначених показників (критеріїв) аудиту [2]. Аудит – форма незалежного, нейтрального контролю будь-якого напряму діяльності широко використовувана на практиці, зокрема у сфері бухгалтерського обліку [3].

Найбільш повним та широким визначенням аудиту можна вважати таке [4]:

Аудит – це форма незалежного, об'єктивного аналізу будь-якої діяльності, або напрямку діяльності, за результатами якого формуються висновки та визначаються перспективні, системні, обов'язкові до виконання плани дій з удосконалення або приведення у відповідність до встановлених критеріїв діяльності або напрямку діяльності, що підлягали аудиту.

Для всіх видів аудиту притаманні три складові: засоби і способи перевірки, результат перевірки та еталон, з яким порівнюється результат перевірки. Розрізняють фінансовий і технічний (промисловий) аудит.

Аудит інформаційної безпеки, як вид технічного аудиту, є важливим з точки зору стратегічного розвитку установи та включає:

– аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки, особливо щодо інформаційних ресурсів;

– оцінку поточного рівня захищеності ІС;

– локалізацію "вузьких місць" в системі захисту ІС;

– оцінку відповідності ІС існуючим стандартам в області інформаційної безпеки;

– надання рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Сьогодні у сфері аудиту формується така практика, що аудит у сфері інформаційних технологій хоча і не має ніякого відношення до фінансового

аудиту, часто є доповненням до нього як комерційної послуги, пропонованої аудиторськими фірмами установам у зв'язку з підвищенням залежності виконання їх завдань і функцій від ІТ та усвідомлення того, що інформація є цінним активом будь-якої установи.

Ідея полягає в тому, що використання надійних і безпечних ІТ систем не тільки до певної міри гарантує надійність фінансової звітності установи, але взагалі становить основу для виконання завдань та функцій, здійснення статутної діяльності, її безперебійного функціонування, стратегічного менеджменту діяльності на майбутнє, фінансового планування.

Головною метою аудиту інформаційної безпеки можна визначити оцінку рівня безпеки ІС установи для управління в цілому з урахуванням перспектив її розвитку. Аудит інформаційних систем є головним і єдиним інструментом перевірки використовуваних установою інформаційних систем, систем безпеки, систем зв'язку з зовнішнім середовищем, корпоративною мережею на предмет їх відповідності бізнес-процесам/ операційним процесам, що провадяться в установі, зокрема відповідності міжнародним стандартам, з подальшою оцінкою ризиків відхилення від еталонної моделі [5]. Аудит інформаційної безпеки базується на ряді принципів [6]. Ці принципи повинні допомогти зробити аудит інформаційної безпеки результативним і надійним інструментом підтримки політик керівництва і засобів управління, надаючи інформацію, яку керівництво установи може задіяти з метою поліпшення результатів діяльності в цілому.

Дотримання цих принципів є необхідною умовою для формування значущих і достатніх висновків аудиту та дозволяє аудиторам, які працюють незалежно один від одного, робити схожі висновки в аналогічних обставинах.

Настанови будь-якого аудиту засновані на таких семи принципах:

1. Бездоганність.
2. Об'єктивне судження.
3. Належна професійна старанність.
4. Конфіденційність.
5.) Незалежність.
6. Підхід, заснований на свідченнях.

7). Ризик-орієнтований підхід.

Аудити можна розділити *за типами* на три групи [7–17].

Аудит першої сторони. Це аудит з ініціативи власника.

Аудит другої сторони. Це аудит з ініціативи контрагента або іншої зацікавленої особи (партнера, співзасновника тощо).

Аудит третьої сторони. Це аудит з ініціативи третьої сторони. До нього відноситься: аудит сертифікаційного органу з метою сертифікації та/або акредитації; аудит на відповідність міжнародним стандартам окремих секторів інформаційної безпеки (GDPR) та діючого внутрішнього та зовнішнього законодавства [20].

Обов'язковий аудит. Коли процедура проведення аудиту затверджена національним законодавством та додатково регулює обов'язковий аудит у важливіших галузях економіки та на стратегічних об'єктах держави (банківська сфера, сфера зв'язку, сфера енергетики, сфера охорони здоров'я, публічні сервіси з наданням персональних даних, інші режимні та стратегічні об'єкти).

До обов'язкового аудиту відносять державний фінансовий аудит використання інформаційних технологій (IT аудит), започаткований у 2020 р. Порядок проведення Державною аудиторською службою, її міжрегіональними територіальними органами державного фінансового аудиту використання інформаційних технологій, затверджений постановою Кабінету Міністрів України від 22.05.2019 р. № 517.

Аудит інформаційної безпеки можна поділити *на види* залежно від критеріїв, за якими відбувається поділ: ***І. За суб'єктом проведення:***

– внутрішній аудит (проводиться штатними спеціалістами відділу/департаменту інформаційної безпеки);

– зовнішній (незалежний експертний) аудит, який може бути змішаним (із залученням як внутрішніх аудиторів/спеціалістів з аудиту інформаційної безпеки та зовнішніх сертифікованих аудиторів, аудиторських фірм, сертифікаційних органів, інших спеціалістів, аутсорсинг).

Зовнішній аудит можна поділити на два типи:

– експертний незалежний аудит;

– сертифікаційний та/або акредитаційний аудит.

Експертний аудит можна умовно уявити як порівняння стану інформаційної безпеки з “ідеальним”/“еталонним” описом, який базується на наступному:

– вимоги, які були пред’явлені керівництвом в процесі проведення аудиту;

– опис “еталонної” системи безпеки, що ґрунтується на акумульованому міжнародному досвіді та досвіді приватного сектору.

При виконанні експертного незалежного аудиту співробітники компанії-аудитора спільно з представниками замовника проводять такі види робіт:

– збір вихідних даних про інформаційну систему, про її функції і особливості, технології автоматизованої обробки і передачі даних (з урахуванням найближчих перспектив розвитку);

– збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення інформаційної безпеки і їх аналіз;

– визначення точок відповідальності систем, пристроїв і серверів ІС;

– формування переліку підсистем кожного підрозділу установи з обробки критичної інформації та схемами інформаційних потоків.

Один із найбільш об’ємних видів робіт, які проводяться при експертному аудиті, є збір даних про інформаційну систему шляхом співбесіди з представниками замовника і заповнення ними спеціальних анкет. Основна мета співбесіди технічних фахівців – збір інформації про функціонування мережі, а керівного складу компанії – з’ясування вимог, які пред’являються до системи інформаційної безпеки.

Необхідно відзначити, що при експертному аудиті інформаційної безпеки ІС враховуються результати попередніх обстежень (в тому числі інших аудиторів), виконуються обробка і аналіз проектних рішень та інших робочих матеріалів, що стосуються питань створення інформаційної системи.

Ключовий етап експертного незалежного аудиту – аналіз проекту інформаційної системи, топології мережі та технології обробки інформації, під час якого виявляються, наприклад, такі недоліки існуючої топології мережі, які знижують рівень захищеності інформаційної системи. За результатами робіт даного етапу пропонуються зміни (якщо вони потрібні) в існуючій інформаційній системі і технології обробки інформації, спрямовані на усунення виявлених недоліків з

метою досягнення необхідного рівня інформаційної безпеки.

Наступний етап – аналіз інформаційних потоків організації. На даному етапі визначаються типи інформаційних потоків ІС установи та складається їх діаграма, де для кожного інформаційного потоку вказуються його цінність (в тому числі цінність переданої інформації) і використовувані методи забезпечення безпеки, що відображають рівень захищеності інформаційного потоку. На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент інформаційної системи, які беруть участь у найбільш важливих процесах передачі, зберігання і обробки інформації.

Для менш цінної інформації рівень захищеності залишається незмінним, що дозволяє зберегти для кінцевого користувача простоту роботи з інформаційною системою. Застосування аналізу інформаційних потоків організації дає можливість спроектувати систему забезпечення інформаційної безпеки, яка відповідає принципу розумної достатності, який полягає в тому, що тільки шляхом прогнозування та своєчасного оцінювання як потенційних загроз і небезпек, так і можливостей впроваджених заходів і засобів захисту можливо ефективно управляти інформаційною безпекою державних установ, забезпечуючи при цьому адекватну динаміку захищеності інформаційних ресурсів при мінімальних економічних витратах [21]. У рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика безпеки, план захисту та різного роду інструкції. Організаційно-розпорядчі документи оцінюються на предмет достатності й несуперечності задекларованим цілям і заходам інформаційної безпеки. Особлива увага на етапі аналізу інформаційних потоків приділяється визначенню повноважень і відповідальності конкретних осіб за забезпечення інформаційної безпеки різних ділянок / підсистем ІС. Повноваження і відповідальність повинні бути закріплені положеннями організаційно-розпорядчих документів. Результати експертного аудиту можуть містити різнопланові пропозиції щодо побудови або модернізації системи забезпечення інформаційної безпеки.

Сертифікаційний та/або акредитаційний аудит (аудит на відповідність стандартам). Суть даного виду аудиту найбільш наближена до тих формулювань і цілей, які існують у фінансовій сфері (див. рис. 1).

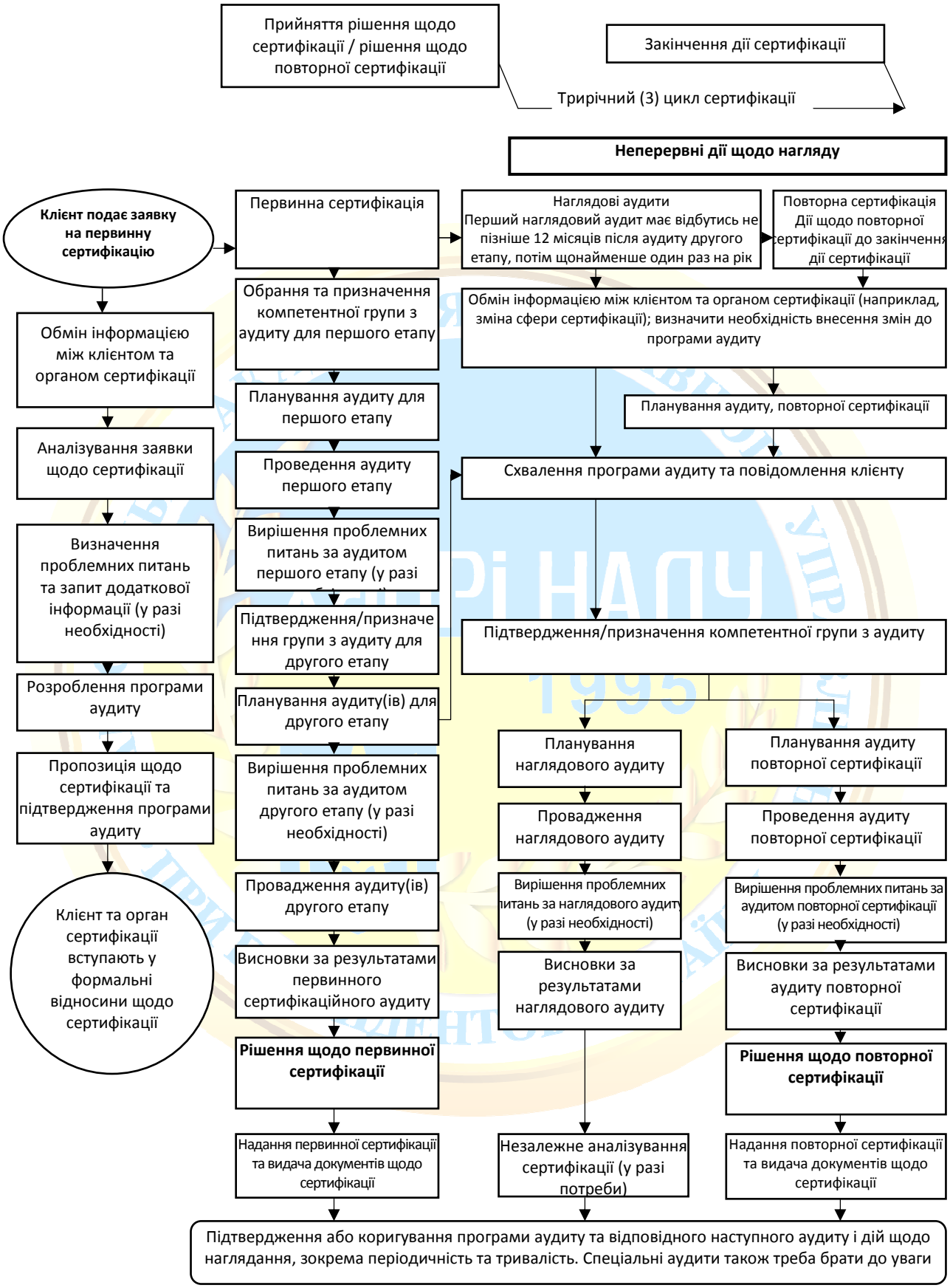

Рис. 1. Блок-схема процесу зовнішнього сертифікаційного аудиту

При проведенні даного виду аудиту стан інформаційної безпеки порівнюється з якимсь абстрактним описом, що приводиться в стандартах. Наразі у світі налічується більш двох десятків стандартів з кібербезпеки та кібераудиту. Актуальним питанням в Україні є створення та розвиток національних стандартів з кібераудиту з використанням/імплементацією кращих міжнародних практик.

Причини проведення аудиту на відповідність стандарту, з подальшою сертифікацією, можна умовно розділити за ступенем обов'язковості даної послуги по відношенню до компанії: обов'язкова сертифікація; сертифікація, викликана "зовнішніми" об'єктивними причинами; сертифікація, що дозволяє отримати вигоди в довгостроковій перспективі; добровільна сертифікація.

Слід зазначити, що у більшості провідних країн світу розроблені стандарти, які застосовуються для сертифікаційного аудиту в обов'язковому порядку для певного виду організацій. Державні організації, відповідно до законодавства багатьох країн зобов'язані проводити атестацію (акредитацію) інформаційно-комунікаційної системи (процедура схожа з сертифікацією) та відповідний аудит кібербезпеки.

II. За імперативністю: обов'язковий та рекомендований (необов'язковий)

Обов'язковий аудит інформаційної безпеки здійснюють підприємства, що відіграють найважливішу роль в економічному секторі країни, зокрема є бюджетоутворюючими, та/або мають стратегічне значення для економіки і безпеки держави. Рекомендований аудит проводиться установами для яких інформація є активом в економічному сенсі. В залежності від цього формується політика інформаційної безпеки та політика аудитів інформаційної безпеки.

III. За зовнішнім проявом: активний або пасивний аудит.

Одним із найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності інформаційної системи з точки зору хакера (або якогось зловмисника, який володіє високою кваліфікацією в області інформаційних технологій).

Найчастіше компанії-постачальники послуг активного аудиту називають його інструментальним аналізом захищеності, щоб відокремити даний вид аудиту від інших.

Суть активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (в тому числі програмно-технічних систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи мережевого захисту.

Під станом системи мережевого захисту розуміються лише ті параметри і налаштування, використання яких допомагає хакеру проникнути у мережу і завдати шкоди установі. Під час здійснення даного виду аудиту інформаційної безпеки на систему мережевого захисту установи моделюється якомога більша кількість мережевих атак, які може виконати хакер. При цьому аудитор штучно створює ті умови, в яких працює хакер: йому надається мінімум інформації, і тільки та інформація, яку можна отримати з відкритих джерел. Звичайно, атаки лише моделюються та не завдають будь-якого деструктивного впливу на інформаційну систему. Різноманітність атак залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора. Результатом активного аудиту є інформація про всі слабкі місця в системі інформаційної безпеки, ступінь їх критичності, методи усунення, відомості щодо широкодоступної інформації (інформація, доступна будь-якому потенційному порушнику) мережі замовника. Після завершення активного аудиту надаються рекомендації щодо модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості і тим самим підвищити рівень захищеності інформаційної системи від дій “зовнішнього” зловмисника при мінімальних витратах на інформаційну безпеку. Однак без проведення у сукупності інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення “ідеальної” системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проекту інформаційної системи.

Активний аудит – послуга, яка може і повинна замовлятися періодично.

Виконання активного аудиту, наприклад, раз на рік, дозволяє упевнитися, що рівень системи мережевої безпеки не знижується. Активний аудит умовно можна розділити на два підвиди – "з моделями зовнішніх порушників та загроз" і "з моделями внутрішніх порушників та загроз". Під час "аудиту із зовнішніми зловмисниками" аудитори моделюють дії "зовнішнього" зловмисника, зокрема моделюються такі процедури:

– визначення доступних з зовнішніх мереж IP-адрес установи;

– сканування даних адрес з метою визначення працюючих сервісів і служб, їх версій, а також призначення відсканованих хостів;

– вивчення маршрутів проходження трафіку до хостів ;

– збір інформації про ІС замовника з відкритих джерел;

– аналіз отриманих даних з метою виявлення вразливостей.

Активний аудит "з моделями внутрішніх порушників та загроз" за складом робіт аналогічний аудиту "з моделями зовнішніх порушників та загроз", однак під час його проведення за допомогою спеціальних програмних засобів моделюються дії "внутрішнього" зловмисника [8].

Найчастіше установа у своїй інформаційній системі використовує спеціалізоване програмне забезпечення (ПО) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, інформаційно-аналітичні системи обробки інформації, автоматизовані робочі місця для виконання визначених завдань та функцій). Подібне програмне забезпечення є унікальним, тому будь-яких готових засобів і технологій для аналізу їх захищеності і відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного програмного забезпечення.

Ще один вид послуг, який останнім часом пропонується найвідомійшими міжнародними практиками під час активного аудиту це ***Пентестинг*** (Pentesting) – дослідження продуктивності та стабільності системи або стрес-тестування. Стрес-тестування спрямоване на визначення критичних точок навантаження, при яких система внаслідок атаки надає відмову в

обслуговуванні запитів користувачів або через підвищену завантаженість перестає адекватно реагувати на легітимні запити користувачів.

Стрес-тест дозволяє виявити “вузькі” місця в процесі формування та передачі інформації і визначити ті умови, при яких нормальна робота системи неможлива. Тестування включає в себе моделювання атак на відмову в обслуговуванні, призначених для користувача запитів до системи, і загальний аналіз продуктивності.

Основна мета даного тестування – демонстрація “успіхів”, яких може досягти хакер, який діє при поточному стані системи мережевого захисту [19]. Результати даної послуги більш наочні, ніж результати аудиту. Однак їй властиві безліч обмежень та особливостей. Наприклад, особливість технічного характеру коли замовник інформується тільки про факт вразливості системи мережевого захисту, в той час як у результатах “зовнішнього” активного аудиту замовнику повідомляються не тільки про факт вразливості мережі, але й відомості про всі слабкі місця і способи їх усунення.

Слід зазначити, що при плануванні перевірки стану системи інформаційної безпеки важливо не тільки точно вибрати вид аудиту, виходячи з потреб і можливостей установи, але й здійснити вибір найбільш кваліфікованого виконавця аудиту. Для того щоб рекомендації на основі аудиту були дійсно об’єктивними, необхідно, щоб аудитор був незалежний у виборі використовуваних систем захисту інформації та мав значний досвід роботи в галузі інформаційної безпеки.

З 2019 р. органи державного фінансового контролю проводять аудит використання інформаційних технологій (IT аудит), складовою частиною якого є оцінка ризиків інформаційної безпеки. Під час проведення IT аудиту органи державного фінансового контролю використовують критерії та індикатори згідно з методологією CobiT® 4.1 (англ. Control Objectives for Information and Related Technology) – відкритого IT-стандарту, розробленого Асоціацією з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (ITGI) з метою оптимізації управління IT: аудитом IT та IT-

безпекою. Державні аудитори самостійно обирають методи, джерела отримання інформації, які відповідають конкретним обставинам проведення IT аудиту [22]. Обрані методи та джерела інформації повинні надавати надійні, необхідні та достатні докази, які підтверджують або спростовують гіпотези аудиту та аудиторські висновки. Державний аудитор одержує інформацію, яку надалі формує в доказову базу, шляхом застосування одного або декількох методів аудиту.

Під час IT аудиту використовуються такі методи:

– анкетування – одержання інформації шляхом письмових відповідей на стандартизовані запитання, які попередньо підготовлені державним аудитором у вигляді бланків-анкет для оцінки законності та ефективності управління публічними коштами, досягнення їх економічного, ефективного та результативного використання;

– аналітичні тести – порівняння інформації та інших даних (показників, індикаторів), як у абсолютних величинах, так і у відносних (індекси, коефіцієнти, відсотки);

– документальна перевірка – перевірка документів і записів, зокрема: візуальна перевірка правильності записів усіх реквізитів, виявлення безпідставних виправлень, підчисток, приписок у тексті й цифрах, перевірка достовірності підписів посадових і матеріально відповідальних осіб; перевірка документів на предмет правильності розрахунків у документах, облікових регістрах і звітних формах; перевірка документів, яка дає змогу встановити законність і доцільність операцій, правильність відображення операцій на рахунках;

– зустрічна звірка – документальне та фактичне підтвердження у підприємств, установ та організацій виду, обсягу і якості операцій для з’ясування їх реальності та повноти відображення в обліку об’єкта аудиту;

– інтерв’ю – одержання інформації шляхом фіксації відповідей на сформульовані запитання державного аудитора;

– перевірка механічної точності – повторна перевірка підрахунків і передачі інформації;

– підтвердження – одержання письмової відповіді, підписаної керівництвом об'єкта аудиту, учасника аудиту для підтвердження точності інформації;

– спостереження – дія, що дає змогу одержати загальну характеристику про хід виконання завдань, заходів, процесів під час використання інформаційних технологій;

– спеціальна перевірка – перевірка, яка здійснюється із залученням кваліфікованих фахівців відповідних органів виконавчої влади, державних фондів, підприємств, установ і організацій (далі – кваліфіковані фахівці) для проведення контрольних обмірів будівельних, монтажних, ремонтних та інших робіт, контрольних запусків сировини і матеріалів у виробництво, контрольних аналізів товарів, інших перевірок, зокрема спрямованих на оцінку надійності ІС в аспектах конфіденційності, цілісності, доступності (безперервності), ідентифікацію загроз, запобігання та управління ризиками;

– фактична перевірка – перевірка кількості та якості майна (ІТ інфраструктури), яка проводиться шляхом обстеження, огляду, обмірювання, перерахунку, зустрічної звірки та інших способів перевірки фактичного стану активів.

У разі встановлення потенційно небезпечних ризиків інформаційної безпеки органи державного фінансового контролю *залучають для надання експертних висновків* сторонніх фахівців з відповідним досвідом, зокрема у сфері кібербезпеки.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямку. З огляду на те, що сьогодні практично вся інформація установи, підприємства, організації сконцентрована в мережі електронних облікових систем, ресурси яких дозволяють підвищити ефективність функціональної діяльності, а використання інформаційних технологій має високий ступінь ризику внутрішнього і зовнішнього втручання в інформаційну архітектуру (нерегламентований внутрішній доступ, відсутність збереження протоколу дій користувача у системі, зовнішнє втручання, зараження вірусами

тощо), зумовлюється збільшення витрат ресурсів через необхідність постійного забезпечення відповідності стану ІТ-складової установи визначеним стратегічним цілям та зовнішньому середовищу.

Як зазначалось у Стратегії кібербезпеки України, затвердженій Указом Президента України від 15.03.2016 р. № 96/2016, загрози кібербезпеці актуалізуються через дію таких чинників:

– невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;

– недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

– недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Саме тому постійно актуалізується вирішення проблеми розвитку аудиту інформаційних систем у світі, удосконалення стандартів, впровадження сертифікації, застосування різних методів та прийомів світових практик аудиту інформаційних систем, а також програмних засобів для проведення аудиту інформаційної безпеки підприємств, установ, організацій усіх форм власності та підпорядкованості, які функціонують у різних галузях економіки та державного управління.

Результати проведення аудиту інформаційних систем дозволяють:

1) виявити значущі загрози для інформації, яка циркулює в установі;

2) зробити оцінку вірогідності настання кожної події, що представляє

загрозу інформаційній безпеці установи, та визначити розмір можливих збитків (шкоди) від наслідків;

3) вдосконалювати політику інформаційної безпеки;

4) створити модель поведінки порушника та класифікувати порушення інформаційної безпеки з визначенням відповідних сценаріїв реагування на загрози інформаційній безпеці;

5) зробити оцінку ефективності впроваджених заходів (інструментів) реагування на загрози інформаційній безпеці;

6) розробити рекомендації з вдосконалення комплексної системи забезпечення інформаційної безпеки установи з обрахунком потреби витрат на поточний момент та на перспективне майбутнє;

7) розробити системні підходи до аудиту інформаційної безпеки установи.

Водночас побудова ефективної ***системи аудиту інформаційної безпеки (як складової частини IT аудиту)***, яка б не лише дозволяла досягти вищезазначених результатів на рівні окремої установи, підприємства, організації, а й забезпечувала б надійний захист від кіберзагроз на рівні інформаційних ресурсів країни, потребує спільних зусиль як ***органів, що здійснюють IT аудит*** (Держаудитслужба, внутрішні аудитори розпорядників бюджетних коштів, суб'єкти аудиторської діяльності, зокрема такі, що спеціалізуються на проведенні кібераудитів), так і ***основних стейкхолдерів у національній системі кібербезпеки***, зокрема Національного координаційного центру кібербезпеки, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України, кіберцентри на рівні міністерств тощо.

При цьому першочергово потребує актуалізації *та подальшого моніторингу змін*, ***інформація стосовно інформаційних систем органів державної влади, місцевого самоврядування, підприємств, установ та організацій державного та комунального сектору економіки***, в тому щодо інформаційних систем об'єктів критичної інфраструктури.

Також на першому етапі необхідно створити законодавче підґрунтя для забезпечення ведення єдиної бази даних інформаційних систем органів державної влади, місцевого самоврядування, підприємств, установ та організацій державного та комунального сектора економіки.

Другий етап – побудова концептуальної моделі ризиків, яка дозволить упереджувати та в режимі реального часу оперативно реагувати на виявлені уразливості інформаційних систем, що призведе до економії витрат на відновлення інформаційних ресурсів та IT інфраструктури.

На третьому етапі – забезпечення проведення за результатами моніторингу ризиків кібербезпеки IT аудиту із залученням відповідних експертів для надання експертних висновків у сфері кіберзахисту.

Відбір інформаційних систем для проведення IT аудитів буде здійснюватися на підставі даних та ризик-орієнтованої єдиної бази даних інформаційних систем, яка буде оперативно оновлюватися органами державної влади, місцевого самоврядування, підприємствами, установами та організаціями.

Знахідки аудиту, відповідні експертні висновки та, як наслідок, рекомендації за результатами аудиту щодо заходів реагування, можна екстраполювати на аналогічні інформаційні системи з метою безпечного функціонування кіберпростору в країні.

Таким чином, система аудиту є важливим механізмом у системі інформаційної безпеки, розвитку кіберпростору як держави в цілому так і окремих державних установ.

Зусилля всіх стейкхолдерів та IT аудиторів повинні бути направлені на розбудову ефективної національної системи кібербезпеки, зокрема гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів; удосконалення нормативно-правової бази щодо аудиту інформаційної безпеки; створення бази знань з профілем кожної IT системи, фіксацією загроз і вразливостей, моделюванням настання загроз та поведінки порушників; розробку вітчизняного

інструментального програмного забезпечення для проведення аудиту інформаційної безпеки.

Список використаних джерел

1. Аверченков В. И. Аудит информационной безопасности : учеб. пособие. 3-е изд., стереотип. Москва : ФЛИНТА, 2016. 269 с.

2. Астахов А. Аудит безопасности информационных систем. Москва, 2012. 79 с.

3. Петренко С. Аудит информационной безопасности корпоративных систем Интернет/Интранет. *Системы безопасности*. 2001. № 41. С. 85–87.

4. Консалтинг і аудит у сфері IT 2004. CNews Analytics. URL: http://www.bezpeka.com (дата звернення: 01.02.2021).

5. Алексеев А. Управление рисками. метод CRAMM, 2015. URL: https://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf (дата звернення: 01.02.2021).

6. Tom Carlson. Information Security Management: Understanding ISO 17799. 2001. URL: http://wisetel.com.br/pe_t-security/biblioteca/referencias_estrangeiras/ISO17799_Whitepaper.pdf (дата звернення: 01.02.2021).

7. ISO 15408 Common Criteria for Information Technology Security Evaluation.. Reference number ISO/IEC 15408-1:2009(E). 2009. URL: https://www.iso.org/standard/40612.html (дата звернення: 01.02.2021).

8. ISO/IEC 27001 Системы обеспечения информационной безопасности. URL: https://www.iso.org/ru/isoiec-27001-information-security.html (дата звернення: 01.02.2021).

9. Cramm. Threat and Risk Management. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення: 01.02.2021).

10. Горбунов А. Практический менеджмент качества. URL: pqm-online.com (дата звернення: 01.02.2021). (дата звернення: 01.02.2021).

11. Міжнародний стандарт ISO/IEC 27001:2013; Cor 1:2014, IDT Information technology – Security techniques – Information security management systems – Requirements. URL: https://www.iso.org/standard/66805.html (дата звернення: 01.02.2021).

12. Міжнародний стандарт ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html (дата звернення: 01.02.2021).

13. Міжнародний стандарт ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security

management systems. URL: https://www.iso.org/standard/62313.html (дата звернення: 01.02.2021).

14. Міжнародний стандарт ISO/IEC 27007:2017 Information technology – Security techniques – Guidelines for information security management systems auditing. URL: https://www.iso.org/standard/67397.html (дата звернення: 01.02.2021).

15. Міжнародний стандарт ISO/IEC 27008:2019 Information technology – Security techniques – Guidelines for the assessment of information security controls. URL: https://www.iso.org/en/standard/61651.html (дата звернення: 01.02.2021).

16. Міжнародний стандарт ISO/IEC 17021-1:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:17021:-1:en (дата звернення: 01.02.2021).

17. Міжнародний стандарт ISO / IEC 19011:2018 Guidelines for auditing management systems. URL: https://www.iso.org/en/standard/70017.html (дата звернення: 01.02.2021).

18. Міжнародний стандарт ISO / IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security. URL: https://www.iso.org/en/standard/46413.html (дата звернення: 01.02.2021).

19. WebTrust. URL: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services (дата звернення: 01.02.2021).

20. GDPR compliance. URL: https://legalitgroup.com/ru/home/ (дата звернення: 01.02.2021).

21. BSI (Агенство Інформаційної Безпеки Німеччини (BSI –- Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency). URL: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html (дата звернення: 01.02.2021).

22. Nessus Network Monitor. URL: Nessus https://www.tenable.com/ (дата звернення: 01.02.2021).

References

1. Averchenkov, V.Y. (2016). Audyt ynformatsyonnoi bezopasnosty. Moscow: Flinta [in Russian].

2. Astakhov, A. (2012). Audyt bezopasnosty ynformatsyonnykh system. Moscow [in Russian].

3. Petrenko, S. (2001). Audyt ynformatsyonnoi bezopasnosty korporatyvnykh system Ynternet/Yntranet. *Systemy bezopasnosty, 41, 85-87* [in Russian].

4. Konsaltynh i audyt u sferi IT 2004. CNews Analytics. URL: http://www.bezpeka.com

[in Ukrainian].

5. Alekseev, A. (2015). Upravlenye ryskamy. Metod CRAMM. URL: https://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf [in Russian].

6. Tom Carlson. (2001). Information Security Management: Understanding ISO 17799. URL: http://wisetel.com.br/pe_t-security/biblioteca/referencias_estrangeiras/ISO17799_ Whitepaper.pdf.

7. ISO 15408 Common Criteria for Information Technology Security Evaluation. Reference number ISO/IEC 15408-1:2009(E). 2009. URL: https://www.iso.org/standard/40612.html.

8. ISO/IEC 27001 Системы обеспечения информационной безопасности. URL: https://www.iso.org/ru/isoiec-27001-information-security.html.

9. Cramm. Threat and Risk Management. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ cramm.html.

10. Gorbunov, A. Praktycheskyi menedzhment kachestva. URL: pqm-online.com [in Russian].

11. ISO/IEC 27001:2013; Cor 1:2014, IDT Information technology – Security techniques – Information security management systems – Requirements. URL: https://www.iso.org/standard/ 66805.html.

12. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html.

13. ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. URL: https://www.iso.org/standard/62313.html.

14. ISO/IEC 27007:2017 Information technology – Security techniques – Guidelines for information security management systems auditing. URL: https://www.iso.org/standard/ 67397.html.

15. ISO/IEC 27008:2019 Information technology – Security techniques – Guidelines for the assessment of information security controls. URL: https://www.iso.org/en/standard/61651.html.

16. ISO/IEC 17021-1:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:17021:-1:en.

17. ISO/IEC 19011:2018 Guidelines for auditing management systems. URL: https://www.iso.org/en/standard/70017.html.

18. ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security. URL: https://www.iso.org/en/standard/46413.html.

19. WebTrust. URL: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services.

20. GDPR compliance. URL: https://legalitgroup.com/ru/home/.

21. BSI (Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency). URL: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html.

22. Nessus Network Monitor. URL: Nessus https://www.tenable.com/.

Plis H. V.,

PhD, Head of the State Audit Office of Ukraine, Kyiv

ORCID 0000-0003-2560-6036;

Kotukh Y. V.,

PhD, Associate Professor of Computer Science, Sumy State University, Sumy

ORCID 0000-0003-4997-620X;

Nekhoroshykh D. M.,

Auditor of Legal Strategy Advisors, Kyiv

ORCID 0000-0002-6455-2221;

Khalimov H. Z.,

Doctor of Technical Sciences, Professor, Head of the Department of Information Technology Security, Kharkiv National University of Radio Electronics, Kharkiv

ORCID 0000-0002-2054-9186 ORCID 0000-0002-2054-9186

Kuchma O. M.,

Head of the Department of Regulatory and Methodological Support of the State Financial Control Process of the State Audit Service of Ukraine, Kyiv

ORCID 0000-0002-7983-7545

Information security audit as a necessary component of management in public institutions

Today, information systems (IS) play a key role in ensuring the efficiency of government agencies, enterprises, organizations.

Government agencies use a variety of IS to store, process and transmit information. This raises the issue of information protection that accumulates, especially given the global trend of increasing the number of information attacks that lead to significant public financial and material

losses. The analysis of information resources demonstrates the transformation of attacks models and patterns of cyber-violators behavior, as priorities change in the objects of attacks, channels of information leakage.

Cybercriminals are developing new software and hardware systems that allow them to carry out more complex and powerful attacks, the organization of which does not require high skills and level of intellectual training. The main purpose of the information security audit can be to assess the level of security of the IS of the institution for management as a whole, taking into account the prospects for its development. Audit of information systems is the main tool to check the information systems used by the institution, security systems, communication systems with the external environment, corporate network for their compliance with business / operational processes carried out in the institution.

Given that today almost all the information of the institution, enterprise, organization is concentrated in a network of electronic accounting systems, resources which increase the efficiency of functional activities, and the use of information technology has a high risk of internal and external interference in information architecture (unregulated internal access, lack of protocol user actions in the system, external intervention, virus infection, etc.), due to increased resource costs taking into account the necessity to constantly ensure compliance with the state of the IT component of the institution to certain strategic goals and the external environment.

As stated in the Cyber Security Strategy of Ukraine, approved by the Decree of the President of Ukraine of March 15, 2016 № 96/2016, cybersecurity threats are actualized due to the action of such factors, in particular, as:

– inconsistency of the electronic communications infrastructure of the state, the level of its development and protection with modern requirements;

– insufficient level of protection of critical infrastructure, state electronic information resources and information, the requirement for protection of which is established by law, from cyber threats; unsystematic measures of cyber protection of critical infrastructure;

– insufficient development of organizational and technical infrastructure for cybersecurity and cyber protection of critical infrastructure and state electronic information resources;

– insufficient effectiveness of the security and defense sector of Ukraine in counteracting cyber threats of military, criminal, terrorist and other nature; insufficient level of coordination, interaction and information exchange between cybersecurity actors.

That is why the solution of the problem of information systems audit development in the world, improvement of standards, introduction of certification, application of various methods and techniques of world information systems audit practices, as well as software for information security audit of enterprises, institutions, organizations of all forms of ownership and subordination

is constantly updated, operating in various sectors of the economy and public administration.

Keywords: cybersecurity; cyber audit; cyber attack; government agencies; government.

Надійшла до редколегії 20.04.2021 р.