УДК 005.254

АНАЛІЗ ВИМОГ МІЖНАРОДНИХ СТАНДАРТІВ ЩОДО ЗДІЙСНЕННЯ АУДИТУ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Клочкова Діана Юріївна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Добринін Ігор Станіславович
кандидат технічних наук, доцент, доцент кафедри інфокомунікаційної інженерії імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. У статті проаналізовані вимоги до проведення аудитів системи менеджменту інформаційної безпеки згідно серії стандартів ISO/IEC 270xx та ISO 19011:2018. Автор робить висновок про вимоги які спрямовані на забезпечення достатнього рівня інформаційної безпеки системи менедженту. На підставі проведеного аналізу визначено головні вимоги до аудитів у сучасних умовах.

Ключові слова: система менеджменту інформаційної безпеки (СМІБ), аудит, внутрішній аудит, організація, аудитор.

Актуальність теми. Міжнародний стандарт інформаційної безпеки ISO/IEC 27001, який увібрав у себе найкращі практики з організації управління інформаційною безпекою та найкращі методи протидії ризикам. Впровадження даного стандарту в національну систему інформаційної безпеки допоможе державі в максимально швидких строках реагувати на різного роду загрози в інформаційному середовищі. Дотримання саме цього стандарту – великий крок до визнання перед світовим товариством а також покращує економічні показники країни. Виходячи з цього, тема роботи є актуальною на сьогодні.

Метою роботи є проведення аналізу вимог стандартів ISO/IEC 270xx та ISO 19011:2018 щодо проведення аудиту інформаційної безпеки.

Виклад основного матеріалу. Аудит - систематичний, незалежний та задокументований процес отримання об’єктивних доказів та їх об’єктивного оцінювання, щоб визначити ступінь дотримання критеріїв аудиту.

Головна мета аудиту інформаційної безпеки - проведення оцінки рівня безпеки інформаційної системи підприємства для управління ним загалом з урахуванням перспектив його розвитку.

Основною метою діяльності організацій є забезпечення необхідного та достатнього рівня ІБ, який є безперервним процесом, та ефективний захист якого неможливий без комплексу організаційних заходів.

Організація повинна оцінювати результативність інформаційної безпеки та ефективність системи управління інформаційною безпекою. Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

Організація повинна проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи система управління інформаційною безпекою: відповідають: власним вимогам організації для її системи управління інформаційною безпекою; та вимогам цього стандарту; ефективно впроваджена та підтримується.

Аудитор повинен перевірити внутрішні аудити СМІБ організації, використовуючи програми та плани аудитів СМІБ, звіти про результати аудиту, плани

дій тощо. Аудитори повинні визначити, наскільки внутрішні аудити СМІБ підтверджують відповідність СМІБ вимогам, визначеним в ISO/IEC 27001, правовим та договірним вимогам, а також іншим вимогам та вимогам СМІБ організації, встановленим внаслідок процесу оцінки ризику.

Організація має бути здатна отримувати максимальну користь із використання доступних ресурсів під час проведення внутрішніх аудитів СМІБ. Організація має встановити процес використання результатів минулих аудитів під час планування майбутніх внутрішніх аудитів СМІБ.

Аудитор СМІБ має бути спроможним сформувати висновок, чи реалізувала організація ефективну програму внутрішнього аудиту СМІБ. Аудитор СМІБ має бути також здатний сформувати висновок, чи справді результати внутрішніх аудитів СМІБ забезпечують адекватні свідчення використання компонентів для вдосконалення процесів СМІБ.

Вище керівництво повинно переглядати систему управління інформаційною безпекою організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності. Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до системи управління інформаційною безпекою. Організація повинна зберігати документовану інформацію як доказ результатів переглядів з боку керівництва.

Процес перевірки, що проводиться керівництвом, не повинен бути заходом, що здійснюється виключно для задоволення вимог стандарту та аудиторів; він має бути інтегральною частиною процесу управління бізнесом організації. Загальна перевірка, що проводиться керівництвом, являє собою складний процес, що здійснюється на різних рівнях організації. Перевірка завжди має бути двостороннім процесом, що виробляється вищим керівництвом за участю всіх рівнів організації.

Аудитори повинні також розглянути, як структуровано керівництво організації та як у цій структурі використовується процес перевірки, що проводиться керівництвом. Записи перевірки, що проводиться керівництвом, необхідні, але їх формат не специфікований. Найпоширенішим видом записів є протоколи нарад, але прийнятними видами записів можуть бути також електронні записи, статистичні діаграми, презентації тощо. буд. не потрібні. Процес перевірки, що проводиться керівництвом, може також включати елементи планування СМІБ, де розглядаються зміни процесів і систем. У цьому випадку аудитори повинні перевірити, чи враховуються такі моменти: - чи оцінюються запропоновані зміни до реалізації; - чи розглядаються питання, пов'язані зі СМІБ, під час підготовки стратегічних планів; - ідентифікуються чи необхідні заходи та засоби контролю та управління до реалізації змін, наприклад, до початку аутсорсингу процесу.

Аудит ІБ повинен проводиться відповідно до вимог стандартів серії ISO/IEC 270xx та ISO 19011:2018.

Треба розробити програму аудиту, яка може охоплювати аудити стосовно одного чи кількох стандартів на системи управління чи стосовно інших вимог, що їх проводять окремо чи в поєднанні (комбінований аудит). Особа, яка керує програмою аудиту, має забезпечити збереження цілісності аудиту, а також унеможливлення надмірного впливу на аудит.

Пріоритет аудиту треба віддавати розподіленню ресурсів та методам так, щоб аудит стосувався питань системи управління з вищим рівнем притаманного ризику та нижчим рівнем дієвості. Для керування програмою аудиту треба призначати компетентних осіб. У програмі аудиту треба подати інформацію та визначити ресурси, які дають змогу результативно й ефективно виконувати аудит у визначені строки. Треба, щоб інформація охоплювала: цілі програми аудиту; ризики та можливості, пов’язані з

програмою аудиту, та дії щодо них; сферу (обсяг, межі, місця розташування) кожного аудиту в межах програми аудиту; графік (кількість/тривалість/періодичність) аудитів; види аудитів, такі як внутрішні чи зовнішні; критерії аудиту; методи аудиту, що їх застосовуватимуть; критерії формування групи аудиторів; перелік відповідної задокументованої інформації.

Частини цієї інформації може не бути в наявності до завершення більш докладного планування аудиту

Потрібно визначити та оцінити ризики та можливості, пов'язані з середовищем функціювання об'єкта аудиту, які можуть стосуватися програми аудиту та можуть вплинути на досягнення її цілей. Особа, яка керує програмою аудиту, має визначити та описати замовнику аудиту ризики та можливості, що їх вона розглядає під час розроблення програми аудиту, а також вимоги щодо ресурсів з тим, щоб їх можна було належно врахувати.

В організації повинні бути визначені ролі та обов'язки осіб. Особі, яка керує програмою аудиту, треба мати необхідну компетентність для результативного та ефективного керування програмою та пов'язаними з нею ризиками та можливостями, а також зовнішніми та внутрішніми чинниками. Особа, яка керує програмою аудиту, має призначити членів групи аудиту, зокрема керівника групи та будь-яких технічних експертів, потрібних для проведення конкретного аудиту та покласти відповідальність за проведення окремого аудиту на керівника групи аудиту.

Повинно бути забезпечене керування результатами виконання програми аудиту та ведення протоколів за програмою аудиту та керування ними.

Особа, яка керує програмою аудиту, має проводити моніторинг програми аудиту. Та разом з замовником аудиту мають проаналізувати програму аудиту, щоб оцінити чи було досягнено її цілей. Досвід, набутий з аналізування програми аудиту, треба використовувати як вхідні дані до процесу поліпшення програми.

Сімейство стандартів ISO/IEC 270xx спрямовані забезпечення достатнього рівня інформаційної безпеки систем менеджменту. Розглянемо докладно вимоги стандартів ISO/IEC 270xx. Стандарт ISO/IEC 27006-2008, заснований на ISO/IEC 17021-2008, задає специфічні вимоги до ряду аспектів, таких як:

1. Вимоги до ресурсів: до компетентності керівництва та персоналу, до персоналу, що бере участь у діяльності з сертифікації, до залучення окремих зовнішніх аудиторів або зовнішніх технічних експертів;

2. Вимоги до інформації: до загальнодоступної інформації, до документів із сертифікації, до посилання на сертифікацію та використання маркування;

3. Вимоги до процесу: до загальних вимог, до початкового аудиту та сертифікації, до діяльності з нагляду, до повторної сертифікації, до спеціальних аудитів, до призупинення, скасування або скорочення сфери дії сертифікації, до апеляцій, до скарг, до документів заявників та клієнтів.

Аудит інформаційної безпеки є основним інструментом контролю за станом захищеності системи менеджменту. Він може виконуватися як у сукупності із загальним аудитом, так і у вигляді самостійного проекту та є невід'ємною частиною забезпечення безпеки інформації.

Висновки. На підставі отриманих результатів можна зробити висновки про те, що сімейство стандартів ISO/IEC 270xx з проведення аудиту інформаційної безпеки спрямовано на забезпечення достатнього рівня інформаційної безпеки СМІБ, підвищує ефективність і забезпечує надійний захист конфіденційних даних. Запропоновані стандартами вимоги до проведення аудиту інформаційної безпеки допомагають забезпечити контроль за якістю виконання плану проведення аудиторської перевірки та регулюють відносини між організаціями та аудиторськими організаціями. При проведенні аудиту СМІБ важливо дотримуватись усіх принципів, описаних у стандарті

ISO 19011 та у серії стандартів ISO/IEC 270xx. Функція аудиту в організації повинна бути незалежною від області, що перевіряється, для отримання об'єктивних результатів.

Список джерел:

1. ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги»
2. ДСТУ ISO/IEC 27006:2015 «Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою».
3. ДСТУ ISO/IEC 27007:2014 «Інформаційні технології. Методи забезпечення безпеки. Керівництво для аудиту систем менеджменту інформаційної безпеки» .
4. ДСТУ ISO 19011:2019 «Настанови щодо проведення аудитів системи управління».