УДК 004.056
DOI: 10.31673/2409-7292.2022.016166

Барсукова К.І.

ПРАВОВІ ЗАСАДИ ТА ЕТАПИ ПОБУДОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

В статті наведено визначення правових засад для побудови ефективної системи захисту інформації шляхом аналізу нормативно-правових актів. Проведено дослідження правових методів забезпечення інформаційної безпеки шляхом аналізу та вивчення комплексної системи захисту інформації та системи управління інформаційною безпекою відповідно до міжнародного стандарту ISO 27001. Наведено опис основних етапів побудови комплексної системи захисту інформації та системи управління інформаційною безпекою, проведено їх порівняння.

Ключові слова: система захисту інформації, система управління інформаційною безпекою, цикл PDCA, правові засади.

Вступ

При побудові системи захисту інформації в Україні необхідно перш за все визначити, яка інформація обробляється за рівнем доступу. Так відповідно до статті 20 Закону України «Про інформацію» інформація за доступом поділяється на:

відкриту інформацію;

інформацію з обмеженим доступом.

Відкрита інформація – це будь-яка інформація, крім тієї, що віднесена законом до інформації з обмеженим доступом. Основними ознаками відкритої інформації є те, що доступ до неї надається будь-яким зацікавленим особам, а будь-яке обмеження права на одержання відкритої інформації забороняється.

Інформацією з обмеженим доступом в свою чергу відповідно до статті 21 Закону України «Про інформацію» є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Таємна інформація - інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Службовою інформацією є інформація, що міститься в документах суб’єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов’язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади.

Разом з тим до інформації з обмеженим доступом не можуть бути віднесені такі відомості:[1]

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Віднесення інформації за рівнем доступу важливо зробити перед початком побудови системи захисту інформації оскільки відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю, а державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх умов які наведено в статті 8 цього закону, однією із яких є підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпеко.

Отже, відповідно до чинного законодавства, для захисту інформації можна будувати комплексну систему захисту інформації з підтвердженою відповідністю або систему управління інформаційною безпекою.

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації. До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та ін.

Для організації робіт зі створення КСЗІ створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

Комплекс засобів захисту (КЗЗ) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Етапи створення КСЗІ

Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів - виконувати одночасно декілька етапів робіт, окремі етапи виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

І етап: Формування загальних вимог до КСЗІ

1.2 Обстеження середовищ функціонування

1.3 Формування завдання на створення КСЗІ

ІІ етап: Розробка політики безпеки інформації в ІТС

2.1 На цьому етапі здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

2.2 Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

2.3 Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002-99 та рекомендаціями НД ТЗІ 1.4-001-2000.

III етап: Розробка технічного завдання на створення КСЗІ

3.1 ТЗ на створення КСЗІ в ІТС є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

3.3 Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:

- у вигляді окремого розділу ТЗ на створення ІТС;
- у вигляді окремого (часткового) ТЗ;

3.4 Перший варіант рекомендується застосовувати для вперше створюваних ІТС. Другий варіант рекомендується застосовувати у випадку модернізації КСЗІ, модернізації діючих ІТС, а також для ІТС, які вже мають затверджене ТЗ на створення, в якому не міститься окремого розділу із захисту інформації.

Вимоги в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 Згідно з цим документом в процесі оцінки захищеності ІТС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

3.7 Для будь-якого варіанту розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати НД ТЗІ 3.7-001-99 та ГОСТ 34.602.

IV етап: Розробка проекту КСЗІ

V етап: Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

Система управління інформаційною безпекою (Information Security Management System, ISMS) – це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов’язки, процедури, процеси і ресурси.[2]

В систему управління інформаційною безпекою, як правило, закладено цикл Демінга(PDCA). PDCA – це простий ітеративний метод керування для перевірки змін у процесах або вирішення проблем та забезпечення їхнього постійного поліпшення з часом. Як і багато методів контролю процесів та якості, що використовуються сьогодні у різних галузях промисловості, цей метод виник з виробничої практики 20-го століття. Простота та відтворюваність PDCA призвели до того, що цей цикл стали використовувати приватні особи, команди або цілі організації у багатьох галузях, не пов'язаних із виробництвом. PDCA було отримано з «циклу Шухарта» Вільяма Едвардса Демінга, названого на честь фахівця зі статистики Волтера Шухарта, якого часто називають батьком сучасного контролю якості. Демінг, американський інженер і професор, набув найбільшої популярності за свою роботу в Японії. Його ідеї вплинули на післявоєнні виробничі процеси та сприяли відновленню країни. Фактично, назва PDCA була придумана учасниками його лекцій, які спростили цикл Шухарта до принципу «плануй, роби, перевіряй, дій». Насправді, Демінг вважав за краще термін «вивчай», а не «перевіряй», відповідно, цикл називався «плануй-роби-вивчай-дій» або PDSA, оскільки в ньому більше уваги приділялося аналізу результатів, а не простої перевірки того, що змінилося.

Цикл PDCA включає 4 етапи: «планування», «виконання», «перевірка» і «дія». Процес виконується лінійно, у своїй завершення одного циклу пов'язані з початком наступного циклу.

Планування. Розуміння вашого поточного та бажаного стану. Простіше кажучи, метою етапу планування є визначення ваших цілей, їх досягнення та оцінка прогресу у їх досягненні. Звичайно, це кілька розпливчастий етап, заснований на тому, що ви намагаєтеся зробити, і різні команди підходять до PDCA по-різному. Хтось може розділити його на кілька проміжних етапів, що вже реалізовано в інших методологіях, таких як DMAIC.

Якщо ви хочете забезпечити ефективне використання можливостей, тоді ваше планування має бути зосереджено на процесах чи діях, необхідних виявлення таких возможностей. Якщо ви хочете вирішити проблему, пов'язану з процесом, то вам може

знадобитися аналіз першопричин, перш ніж ви зможете розпочати реалізацію плану. У будь-якому випадку використання даних, будь то вже існуючі дані процесу або аналіз попередніх циклів PDCA, допоможе вам розробити план дій або гіпотезу.

Виконання. Як тільки у вас з'явиться план дій або потенційне вирішення проблеми, протестуйте їх. Етап виконання – це час, протягом якого ви можете протестувати свої початкові запропоновані зміни. Однак його слід розглядати як експеримент, оскільки час для повного впровадження рішення чи зміни процесу ще не настав. Таким чином, цей етап слід проводити в невеликих масштабах та в контрольованій обстановці. На нього не повинні впливати зовнішні фактори, і він не повинен порушувати інші процеси та дії вашої робочої групи чи організації. Звичайно, весь зміст цього етапу полягає в зборі даних та інформації про результати тесту, тому що на цьому будуть ґрунтуватися наступні етапи процесу.

Перевірка. Після завершення тестування вам необхідно оцінити, чи принесли запропоновані вами зміни чи рішення очікуваний ефект. На етапі перевірки ви аналізуєте дані, зібрані на етапі виконання, та порівнюєте їх зі своїми початковими цілями та завданнями. Також слід оцінити підхід до тестування, який ви використовуєте, щоб зрозуміти, чи були внесені будь-які зміни в метод, визначений на етапі планування, які могли вплинути на процес. Загалом завдання цього етапу — оцінити, наскільки успішним є ваш результат і що слід зробити на наступному етапі процесу. Насправді, ви можете провести інший тест, повторюючи етапи виконання та перевірки, доки не знайдете задовільне рішення для переходу на етап дії.

Дія. Після закінчення циклу ви разом із учасниками робочої групи повинні визначити зміни, які, можливо, будуть впроваджені у процес. Однак PDCA називається циклом недарма, оскільки будь-які зміни, які вносяться вами в етап дії, не є завершенням процесу. Ваш новий та покращений продукт, процес чи вирішена проблема повинні сформувати нову основу для подальших повторень циклу PDCA.

Команди та спеціалісти-практики PDCA зазвичай з'ясовують, які інструменти виявилися найефективнішими на кожному етапі. Однак, незалежно від того, проводите ви мозкові штурми на етапі планування або збираєте дані на етапі перевірки, Dropbox Paper допоможе вам в управлінні кожною частиною процесу. Загальні документи з планування проекту допомагають намітити процес, у той час як інструменти для спільної роботи підтримують залучення робочої групи і допомагають їй слідувати плану-графіку при повторенні циклу PDCA. І, звичайно, всі ваші документи — це файли, якими можна легко ділитися через сховище Dropbox .

Тим не менш, сьогодні цей метод найбільш відомий як цикл PDCA, тому що він передбачає виконання та багаторазове повторення дій. Структуру та логіку можна побачити і в інших методах управління якістю на виробництві, таких як «ощадливе виробництво», «кайдзен» та «шість сигм».

Найбільш значущою метою більшості систем інформаційної безпеки є захист бізнесу та знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації.

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов’язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей.

Досягнення заданих цілей можливо у ході вирішення таких основних завдань, як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки та проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної

безпеки, у тому числі методи їх оцінки, контролю інформаційної безпеки на підприємстві. Слід зазначити, що тут перераховано не повний список.[2]

Побудова СУІБ дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування, і т.д.

Основні функції системи управління інформаційною безпекою:

виявлення та аналіз ризиків інформаційної безпеки;

планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

контроль цих процесів;

внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління інформаційною безпекою базується на наступних принципах: [2]

комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі підприємства та за її межами;

узгодженість з бізнес-задачами і стратегією підприємства;

високий рівень керованості;

адекватність інформації, яка використовується і генерується;

ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

безперервність управління;

процесний підхід – зв'язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв'язку між етапами.

Одним з ключових чинників успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC 27001.

Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

СУІБ забезпечує вибір адекватних і пропорційних методів і засобів контролю та захисту інформації і, тим самим, довіру зацікавлених сторін.

Проте слід брати до уваги й інші стандарти в сфері інформаційної безпеки. На даний момент у світовій практиці використовується велика кількість стандартів, методик та інших документів, що регламентують процеси управління інформаційною безпекою, наприклад ISM3, COBIT, ITIL / ITSM, BSI-100-2, ISO13335-4, CRAMM, ISO15408. Але варто відмітити, що всі вони сумісні з ISO 27001, а також подобні до нього.[2]

Етапи побудови СУІБ

І етап: Визначення області дії СУІБ

ІІ етап: Попередній аудит на відповідність вимогам ISO 27001:

збір вихідних даних про бізнес-процеси, структурні підрозділи, інформаційно-телекомунікаційну інфраструктуру, методи і засоби забезпечення інформаційної безпеки;

аналіз діючої організаційно-розпорядчої документації, що регламентує питання забезпечення інформаційної безпеки;

оцінка поточного рівня відповідності вимогам стандарту ISO 27001.

ІІІ етап: Проведення оцінки ризиків:

Розробка методики оцінки ризиків;

Інвентаризація та класифікація активів;

Формування карти загроз;

Аналіз і оцінка ризиків;

Розробка плану обробки ризиків.

IV етап: Розробка процедур і документації СУІБ:

Розробка процесів управління інформаційною безпекою;

Розробка процесів забезпечення інформаційної безпеки;

Розробка комплекту організаційно-розпорядчої документації, що регламентує питання забезпечення інформаційної безпеки;

Розробка програм підвищення обізнаності з питань управління та забезпечення інформаційної безпеки;

V етап: Впровадження процедур і документації СУІБ:

Впровадження процесів управління інформаційною безпекою;

Впровадження процесів забезпечення інформаційної безпеки;

Навчання та підвищення обізнаності співробітників в області забезпечення інформаційної безпеки.

VI етап:. Дослідна експлуатація СУІБ

VII етап: Сертифікаційний аудит і видача міжнародного сертифікату:

Взаємодія з органом сертифікації;

Консультаційна підтримка при проходженні сертифікаційного аудиту.

Результатом робіт є СУІБ компанії, що відповідає вимогам стандарту ISO 27001.

За результатами дослідження можна прийти до висновку, що комплексна система захисту інформації робить акцент на захисті інформації шляхом захисту та набору правил для інформаційних систем, та може складатися з окремих модулів з збереженням обміну інформацією. Основним недоліком даної системи є те, що у разі внесення змін, потрібно створювати нову систему захисту інформації з отриманням нового експертного висновку. В свою чергу, система управління інформаційною безпекою орієнтована за захист інформації в системі та бізнес процесів в цілому, та, за бажанням, операційних процесів, які забезпечують діяльність організації в цілому, навіть перевірку постачальників. Можливо отримати міжнародний сертифікат відповідності. У разі необхідності внесення змін виконується оцінка ризиків для зміненого процесу та внесення змін до заходів безпеки та здійснення внутрішнього аудиту, за необхідності зовнішнього. Для ефективного функціонування потрібен постійний моніторинг функцій СУІБ, контроль процесу інцидентами, внутрішній аудит 2 рази на рік та зовнішній кожних два роки, або після внесення суттєвих змін, залучення керівництва на всіх етапах, виконання оцінки ризиків 1 раз в рік, постійне навчання працівників з тренінгами, курсами, лекціями та перевіркою знань.

Висновок

Отже, відповідно до чинного законодавства, для захисту інформації можна будувати комплексну систему захисту інформації з підтвердженою відповідністю для інформації з обмеженим доступом та державних інформаційних ресурсів обов'язкової та відкритої інформації, або систему управління інформаційною безпекою відповідно для відкритої інформаційної безпеки. Також слід звернути увагу, що побудова комплексної системи захисту інформації є майже безкоштовною, але з великою кількістю бюрократичної роботи. В свою чергу, система управління інформаційною безпекою, у разі отримання сертифікату відповідності, має високу вартість та вимагає залучення зовнішніх аудиторів.

Перелік посилань

1. Науково-практичний коментар Закону України «Про запобігання корупції». - Київ: Юрінком Інтер, 2020. - 348 с.

2. Система управління інформаційною безпекою як ключовий чинник успішності організації[Електронний ресурс]// - Режим доступу: https://ua.ikmj.com/isms/ (24.05.2022).

Надійшла: 14.01.2022 Рецензент: д.т.н., доцент Ахрамович В.М.